Universal Management Suite (UMS)

IGEL Universal Management Suite (UMS) ist eine Managementsoftware für die sichere zentrale Fernadministration von IGEL OS-Geräten. Mit der UMS können Sie Endgeräte genauso konfigurieren wie lokal am Gerät. Einen allgemeinen Überblick über die UMS finden Sie unter Überblick über die IGEL UMS (see page 238).

Installation und Konfiguration

UMS Installieren und Aktualisieren (see page 245), Leitlinien zur Installation und Größenbestimmung der IGEL UMS (see page 279), Verbindung zur UMS (see page 319), Benutzerverwaltung (see page 672), UMS Administration (see page 549)

Lizenzen

Automatic License Deployment, UMS Lizenzen (see page 561), Gerätelizenzen (see page 562)

Endgerätebereitstellung

Geräte registrieren (see page 322)

Benutzerhilfe

Support Information (see page 352), Nachrichten (see page 359), Logging (see page 661)

Endgerätekonfiguration

Profile verwenden (see page 371), Priority Profile (see page 413), Templateprofile (see page 416), Wirksamkeit der Einstellungen (see page 370)

Firmwareverwaltung

Firmwareupdate (see page 539), Firmwares exportieren (see page 468), Firmwares importieren (see page 469), Suche nach neuen Universal-Firmware-Updates (see page 540)

Individuelle Gestaltung

Themen (see page 349), Firmwareanpassung (see page 435)

Views und Suche

Quick Search (see page 363), Views (see page 489), Suche mit regulären Ausdrücken (see page 231)

Artikel zur UMS

Geräte, die von der IGEL Universal Management Suite (UMS) unterstützt werden

Frage

Welche Geräte werden von der IGEL Universal Management Suite (UMS) unterstützt?

Antwort

⚠ Um sicherzustellen, dass Sie alle neuen Features von IGEL OS nutzen können:

- ▶ Aktualisieren Sie Ihre UMS auf die neueste Version.
- ▶ Wählen Sie bei allen relevanten OS 11-Profilen (see page 372) für **Basiert auf** die passende Firmwareversion.
- ▶ Für OS 12-Profile (see page 838) ist Folgendes zu beachten: Ein OS 12-Profil konfiguriert ALLE Versionen einer App, solange nicht eine bestimmte Version unter **Versionen anzeigen** festgelegt ist.

Die neueste UMS Version unterstützt folgende Funktionen

- alle IGEL Geräte, die Ihr Ende der Maintenance noch nicht erreicht haben
- Geräte, die mit IGEL OS Creator (OSC) konvertiert wurden

Unterstützung für ältere UMS-Versionen

- IGEL Geräte, die vor der UMS Version freigegeben wurden
- und die zum Zeitpunkt des UMS Release noch nicht ihr Ende der Maintenance erreicht hatten

IGEL UMS Kommunikationsports

Die folgende Tabelle zeigt welche Standardports von den Komponenten der IGEL Universal Management Suite (UMS) und einer UMS Infrastruktur verwendet werden. Einige dieser Ports sind konfigurierbar, z. B. Web-Server-Port 8443, Gerätekommunikationsport 30001 für IGEL OS 11-Geräte usw. (siehe Einstellungen - Servereinstellungen im IGEL UMS Administrator ändern (see page 709)).

Port (Protokoll)	Erforderlich für UMS Feature	Wer lauscht? Applikationen/ Bindung von Diensten an den Port	Wer spricht? Anwendungen/ Dienst, die die Kommunikation initiieren	Beschreibung
443 (TCP)	IGEL App Portal https://app.igel.com/	Cloud Service	UMS Server	Der UMS Server importiert Apps vom IGEL App Portal.
443 (TCP)	IGEL Onboarding Service https://obs.services.igel.com[1]	Cloud Service	UMS Server	Der UMS Server validiert das Onboarding-Token.
443 (TCP)	IGEL Insight Service https://insight.services.igel.com	Cloud Service	UMS Server	Der UMS Server überträgt Analyse- und Nutzungsdaten an IGEL.
443 (TCP)	Automatic License Deployment (ALD)	IGEL Lizenzserver (unter susi.igel.com)	UMS Server	Der UMS Server fordert Lizenzen an; siehe UMS Kontaktaufnahme mit dem Lizenzserver (see page 63).

1 https://obs.services.igel.com/

Port (Protokoll)	Erforderlich für UMS Feature	Wer lauscht? Applikationen/ Bindung von Diensten an den Port	Wer spricht? Anwendungen/ Dienst, die die Kommunikation initiieren	Beschreibung
443 (TCP)	Automatic License Deployment (ALD)	IGEL Downloadserver (HTTP-Server unter fwus.igel.com)	UMS Server	Der UMS Server erfragt die Verbindungsdetails, die für die Verbindung zum IGEL Lizenzserver erforderlich sind (unter susi.igel.com). Siehe UMS Kontaktaufnahme mit dem Lizenzserver (see page 63).
8443 (TCP)	Core	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	UMS Konsole / UMS Web App	Siehe UMS mit interner Datenbank (see page 24) oder UMS mit externer Datenbank (see page 25).

Port (Protokoll)	Erforderlich für UMS Feature	Wer lauscht? Applikationen/ Bindung von Diensten an den Port	Wer spricht? Anwendungen/ Dienst, die die Kommunikation initiieren	Beschreibung
8443 (TCP)	Unified Protocol	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 12-Gerät	Das Gerät öffnet einen WebSocket zum Datenaustausch (gesamte Kommunikation inkl. Registrierung über IGEL Onboarding Service oder One-Time-Password-Methode, Dateitransfer, Firmwareanpassung und Lizenzübertragung, sicheres Spiegeln, sicheres Terminal) Weitere Informationen zum Unified Protocol finden Sie unter Überblick über die IGEL UMS (see page 238).
8443 (TCP)	UMS as an Update Proxy	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 12-Gerät	Das Gerät kontaktiert den UMS Server, um App-Updates herunterzuladen.

Port (Protokoll)	Erforderlich für UMS Feature	Wer lauscht? Applikationen/ Bindung von Diensten an den Port	Wer spricht? Anwendungen/ Dienst, die die Kommunikation initiieren	Beschreibung
30002 (TCP)	Core (direkt, ohne ICG)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	HA Load Balancer	Wenn der UMS Server und der HA Load Balancer auf demselben Host laufen, verwendet der UMS Server den Port 30002 anstelle von 30001 und der HA Load Balancer den Port 30001 (nur für IGEL OS 11 relevant).
30001 (TCP)	Unified Protocol (automatische Registrierung oder Registrierung nach dem Scannen)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 12-Gerät	Das Gerät fordert ein Registrierungstoken an, wenn der UMS Server im Unternehmensnetzwerk erkannt wurde (siehe Geräte automatisch an der IGEL UMS registrieren (see page 337) und Geräte importieren (see page 331)) oder das Gerät eine Registrierungsanfrage nach dem Scannen erhalten hat (siehe Netzwerk nach Geräten scannen und Geräte an der IGEL UMS registrieren (see page 324)).

Port (Protokoll)	Erforderlich für UMS Feature	Wer lauscht? Applikationen/ Bindung von Diensten an den Port	Wer spricht? Anwendungen/ Dienst, die die Kommunikation initiieren	Beschreibung
30001 (TCP)	Core (direkte Gerätekommunikation, nicht bei Kommunikation über ICG verwendet)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11-Gerät	Siehe Geräte kontaktieren die UMS (see page 32).
8443 (TCP)	Core (Datentransfer)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11-Gerät	Das Gerät fordert eine Datei von der UMS an; siehe UMS und Geräte: Dateiübertragung (see page 55).
8443 (TCP)	Core (Firmwareanpassungen)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11-Gerät	Die UMS stellt Dateien zur Verfügung, mit denen das Erscheinungsbild der Benutzeroberfläche des Geräts angepasst werden kann; siehe UMS und Geräte: Dateiübertragung (see page 55).
88 (TCP/ UDP)	Core (bei Verwendung von Active Directory), Shared Workplace	MS Active Directory Service	UMS Server	Der UMS Server sendet eine Kerberos-Anfrage an MS Active Directory.
389 (TCP)	Core (bei Verwendung von Active Directory), Shared Workplace	MS Active Directory Service	UMS Server	Der UMS Server sendet eine LDAP-Anfrage an MS Active Directory.

Port (Protokoll)	Erforderlich für UMS Feature	Wer lauscht? Applikationen/ Bindung von Diensten an den Port	Wer spricht? Anwendungen/ Dienst, die die Kommunikation initiieren	Beschreibung
1527 (TCP)	Core (wenn Apache Derby verwendet wird)	Apache Derby Datenbank (Derby Network Server)	UMS Server	Siehe UMS mit externer Datenbank (see page 25).
636 (TCP)	Core (wenn ein LDAPS Server verwendet wird)	LDAPS-Server (anders als MS Active Directory)	UMS Server	Der UMS Server sendet eine LDAP-Anfrage über SSL.
1433 (TCP)	Core (wenn MS SQL Server verwendet wird)	Microsoft SQL Server Datenbank	UMS Server	Siehe UMS mit externer Datenbank (see page 25).
1521 (TCP)	Core (wenn Oracle verwendet wird)	Oracle Datenbank	UMS Server	Siehe UMS mit externer Datenbank (see page 25).
5432 (TCP)	Core (wenn PostgreSQL verwendet wird)	PostgreSQL Datenbank	UMS Server	Siehe UMS mit externer Datenbank (see page 25).
8443 (TCP)	Core (Lizenzen)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11-Gerät	Die UMS stellt Lizenzdateien für die Geräte zur Verfügung; siehe UMS und Geräte: Dateiübertragung (see page 55).
Auto ("high port") (UDP)	Core (Online Check)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11-Gerät	Das Gerät reagiert auf eine von der UMS gesendete Nachricht, um zu prüfen, ob das Gerät online ist. Die Nummer des zu verwendenden Ports ist in dem von der UMS gesendeten UDP-Paket enthalten.

Port (Protokoll)	Erforderlich für UMS Feature	Wer lauscht? Applikationen/ Bindung von Diensten an den Port	Wer spricht? Anwendungen/ Dienst, die die Kommunikation initiieren	Beschreibung
30005 (TCP/ UDP)	Core (Scannen nach Geräten)	Gerät (OS 12 & OS 11) (UMS Agent)	Gerät (OS 12 & OS 11)	Das Gerät reagiert auf einen Broadcast, der von der UMS während eines Scans gesendet wird. Die Nummer des zu verwendenden Ports ist in dem von der UMS gesendeten UDP-Paket enthalten. Siehe UMS Server (see page 238).
Auto ("high port") (UDP)	Core (Scannen nach Geräten)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Gerät (OS 12 & OS 11)	Das Gerät reagiert auf einen Broadcast, der von der UMS während eines Scans gesendet wird. Die Nummer des zu verwendenden Ports ist in dem von der UMS gesendeten UDP-Paket enthalten.
30022 (TCP)	Core (sicheres Terminal)	IGEL OS 11-Gerät (UMS Agent)	UMS Server	Siehe UMS und Geräte: Sicheres Terminal (see page 50).
5900 (TCP)	Core (Spiegeln)	IGEL OS 11-Gerät (UMS Agent)	UMS Konsole	Die UMS Konsole initiiert eine VNC-Sitzung für die Spiegelung; siehe UMS und Geräte: Spiegeln (see page 36).

Port (Protokoll)	Erforderlich für UMS Feature	Wer lauscht? Applikationen/ Bindung von Diensten an den Port	Wer spricht? Anwendungen/ Dienst, die die Kommunikation initiieren	Beschreibung
5900 (TCP)	Core (Spiegeln) via UMS Web App	IGEL OS 11-Gerät (UMS Agent)	UMS Server	Die UMS Web App veranlasst den UMS Server, eine VNC-Sitzung für das Spiegeln zu initiieren. Die VNC-Sitzung wird durch den UMS Server geroutet; siehe UMS und Geräte: Spiegeln (see page 36).
9080 (TCP)	Core (unverschlüsselt, kein SSL)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11-Gerät	Das Gerät fordert von der UMS eine Datei an (normaler Dateitransfer oder Universal Firmware Update). Dieser Port wird nur dann verwendet, wenn **Nur SSL-Verbindungen zulassen** im UMS Administrator deaktiviert ist. Wenn **Nur SSL-Verbindungen zulassen** aktiviert ist, wird Port 8443 für Firmware-Updates und Dateiübertragung verwendet.

Port (Protokoll)	Erforderlich für UMS Feature	Wer lauscht? Applikationen/ Bindung von Diensten an den Port	Wer spricht? Anwendungen/ Dienst, die die Kommunikation initiieren	Beschreibung
Auto ("high port")	Core (unverschlüsselt, kein SSL)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	UMS Konsole	Die GUI wird über die Java Webstart Konsole gestartet. Dieser Port wird nur dann verwendet, wenn **Nur SSL-Verbindungen zulassen** im UMS Administrator deaktiviert ist. Wenn **Nur SSL-Verbindungen zulassen** aktiviert ist, wird Port 8443 für Firmware-Updates und Dateiübertragung verwendet.
443 (TCP)	Core (Universal Firmware Update)	IGEL Downloadserver (HTTP-Server at fwus.igel.com)	UMS Server	Siehe UMS kontaktiert den Downloadserver, um nach neuen Updates zu suchen (see page 57).
8443 (TCP)	Core (Universal Firmware Update)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11-Gerät	Im Rahmen eines Universal Firmware Updates fordert das Gerät eine Datei von der UMS an; siehe UMS und Geräte: Dateiübertragung (see page 55).
9 (UDP)	Core (Wake on LAN)	Gerät (OS 12 & OS 11)	UMS Server	Der UMS Server sendet "magic" Pakete an die Geräte.

Port (Protokoll)	Erforderlich für UMS Feature	Wer lauscht? Applikationen/ Bindung von Diensten an den Port	Wer spricht? Anwendungen/ Dienst, die die Kommunikation initiieren	Beschreibung
8443 (TCP)	Core (mit ICG)	ICG (IGEL Cloud Gateway)	UMS Server	Siehe Geräte und UMS Server kontaktieren sich über ICG (see page 29) oder UMS Server (see page 238).
8443 (TCP)	Core (mit ICG)	ICG (IGEL Cloud Gateway)	Gerät (OS 12 & OS 11)	Siehe Geräte und UMS Server kontaktieren sich über ICG (see page 29).
6155 (UDP)	High Availability (HA)	HA Load Balancer UMS Server	HA Load Balancer UMS Server	Der HA Load Balancer und der UMS Server lauschen auf Port 6155 und verwenden diesen für die Kommunikation.
8443 (TCP)	High Availability (HA) und Distributed UMS	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Dateisynchronisation zwischen UMS Servern.
61616 (TCP/ UDP)	High Availability (HA)	HA Load Balancer UMS Server	HA Load Balancer UMS Server	Sowohl HA Load Balancer als auch UMS Server lauschen auf Port 61616 und verwenden ihn zur Kommunikation.

Port (Protokoll)	Erforderlich für UMS Feature	Wer lauscht? Applikationen/ Bindung von Diensten an den Port	Wer spricht? Anwendungen/ Dienst, die die Kommunikation initiieren	Beschreibung
8443 (TCP)	IMI	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Komponente eines Drittherstellers, die IMI (IGEL Management Interface) verwendet	Siehe IGEL Management Interface (IMI) (see page 27).

IGEL Universal Management Suite Network Configuration

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Configure the UMS for Integrating Reverse Proxy with SSL Offloading

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

NGINX: Example Configuration for as Reverse Proxy in IGEL OS with SSL Offloading

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

F5 BIG IP: Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Azure Application Gateway: Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Citrix Netscaler: Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

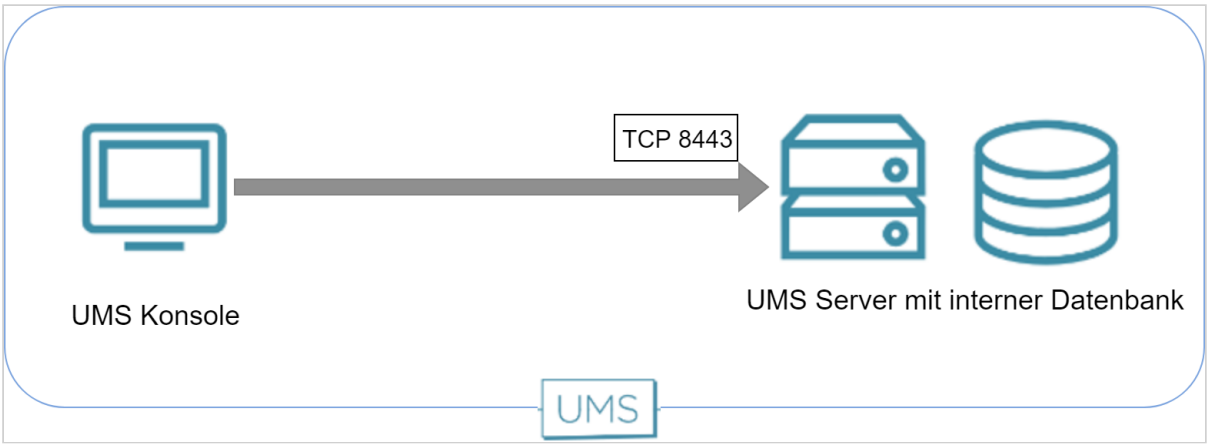
Interne Kommunikation

UMS mit interner Datenbank

Die Kommunikation zwischen der UMS Konsole und dem UMS Server findet über HTTPS statt. Standardmäßig achtet der UMS Server auf Anfragen auf dem TCP-Port 8443. Der Port kann unter **UMS Adiministration** unter **Einstellungen > GUI-Serverport** geändert werden.

Der von der UMS für interne TCP-Anfragen an die Embedded-Datenbank verwendete Port kann im UMS Administrator unter **Einstellungen > Datenbank-Port (Embedded DB)** geändert werden. Der Standard-Port ist 1528.

Die folgende Abbildung veranschaulicht die Kommunikation zwischen den UMS-Komponenten:



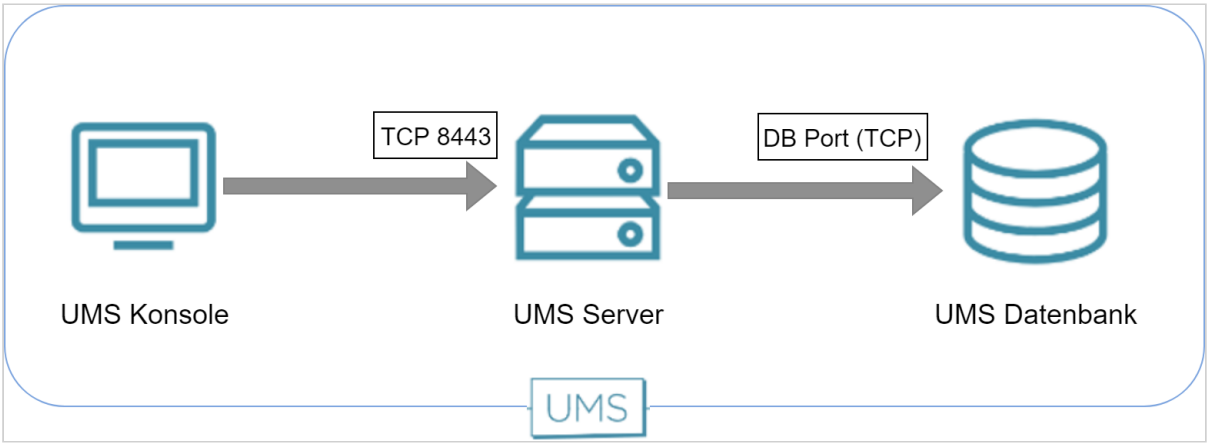
UMS mit externer Datenbank

Die Kommunikation zwischen der UMS Konsole und dem UMS Server erfolgt über HTTPS. Standardmäßig hört der UMS-Server TCP-Anfragen auf Port 8443 ab. Der Port kann im UMS Administrator unter **Einstellungen > GUI Server Port** geändert werden.

Die von der UMS für TCP-Anfragen an die Datenbank verwendeten Ports sind wie folgt definiert:

Datenbanktyp	Datenbank-Port (Standard)	Konfiguration
Apache Derby (Derby Netzwerk Server)	1527	(UMS Administrator) **Datenquelle >Hinzufügen... >** [wählen Sie **Derby** als DB-Typ] **> Port**
MS SQL Server	1433	(UMS Administrator) **Datenquelle > Hinzufügen... >** [wählen Sie **SQL Server** als DB-Typ] **> Port**
Oracle	1521	(UMS Administrator) **Datenquelle > Hinzufügen... >** [wählen Sie **Oracle** als DB-Typ] **> Port**
PostgreSQL	5432	(UMS Administrator) **Datenquelle > Hinzufügen... >** [wählen Sie **PostgreSQL** als DB-Typ] **> Port**

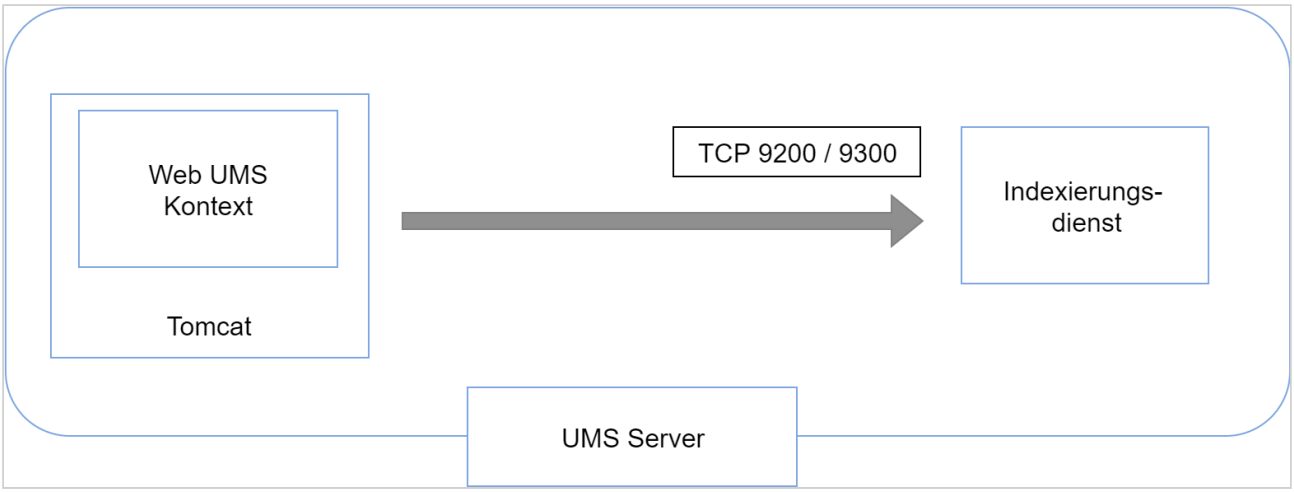
Die folgende Abbildung veranschaulicht die Kommunikation zwischen den UMS-Komponenten:



Indizierung für die Suchfunktion der UMS Web App

Der Indexierungsdienst, der von der Suchfunktion der UMS Web App verwendet wird, lauscht auf den Ports 9200 und 9300. Der Web UMS Kontext liest und schreibt Daten über diese Ports. Die Ports sind intern offen, können aber nicht von außerhalb des UMS Servers erreicht werden.

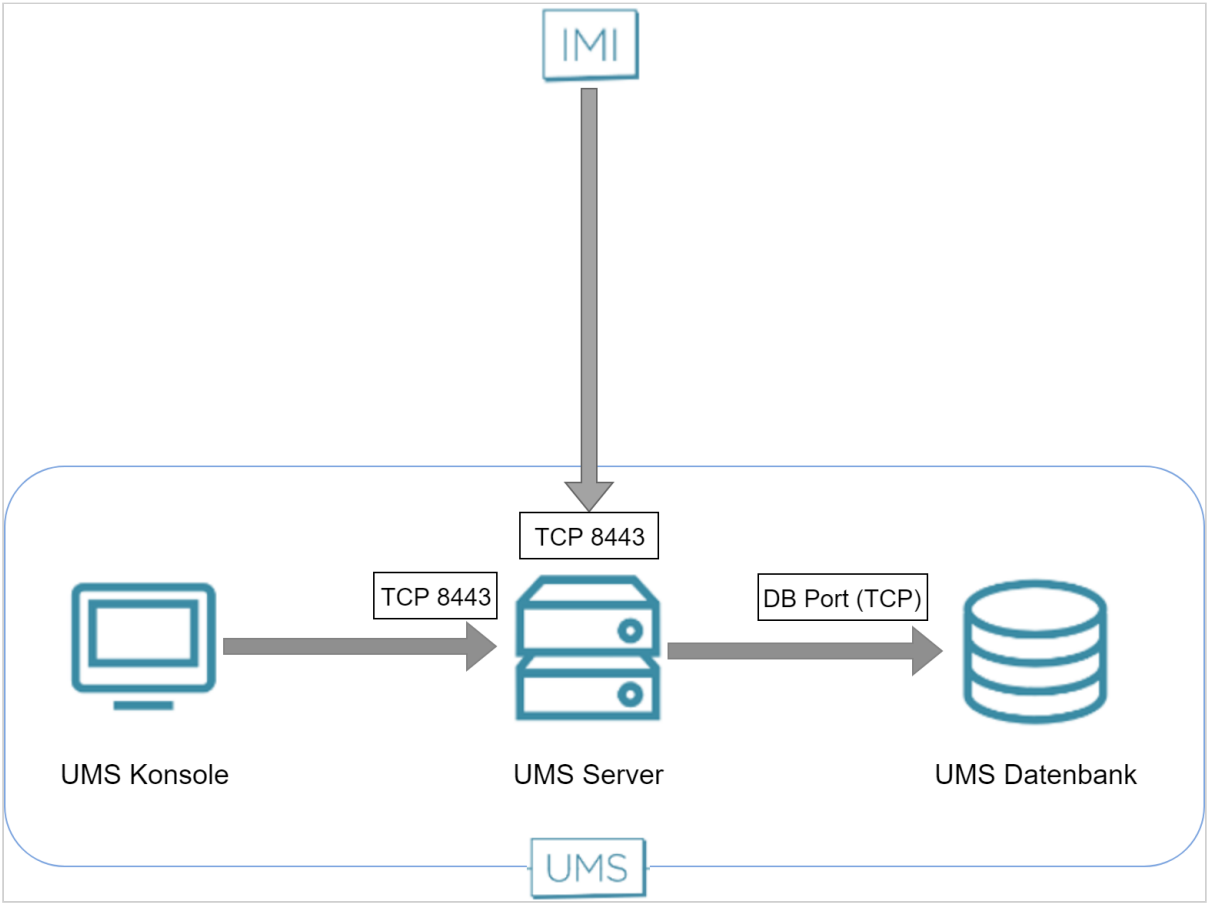
Die folgende Abbildung veranschaulicht die Kommunikation innerhalb des UMS Servers:



IGEL Management Interface (IMI)

Die vom IGEL Management Interface bereitgestellte REST-API wird über HTTP auf Port 8443 (TCP) bereitgestellt.

Die folgende Abbildung veranschaulicht die Kommunikation mit dem UMS-Server über IMI:



UMS und Geräte: Einstellungen und Kontrolle

Geräte und UMS Server kontaktieren sich über ICG

Um mit der UMS zu kommunizieren, initiieren die Geräte eine TCP-Verbindung zum ICG.

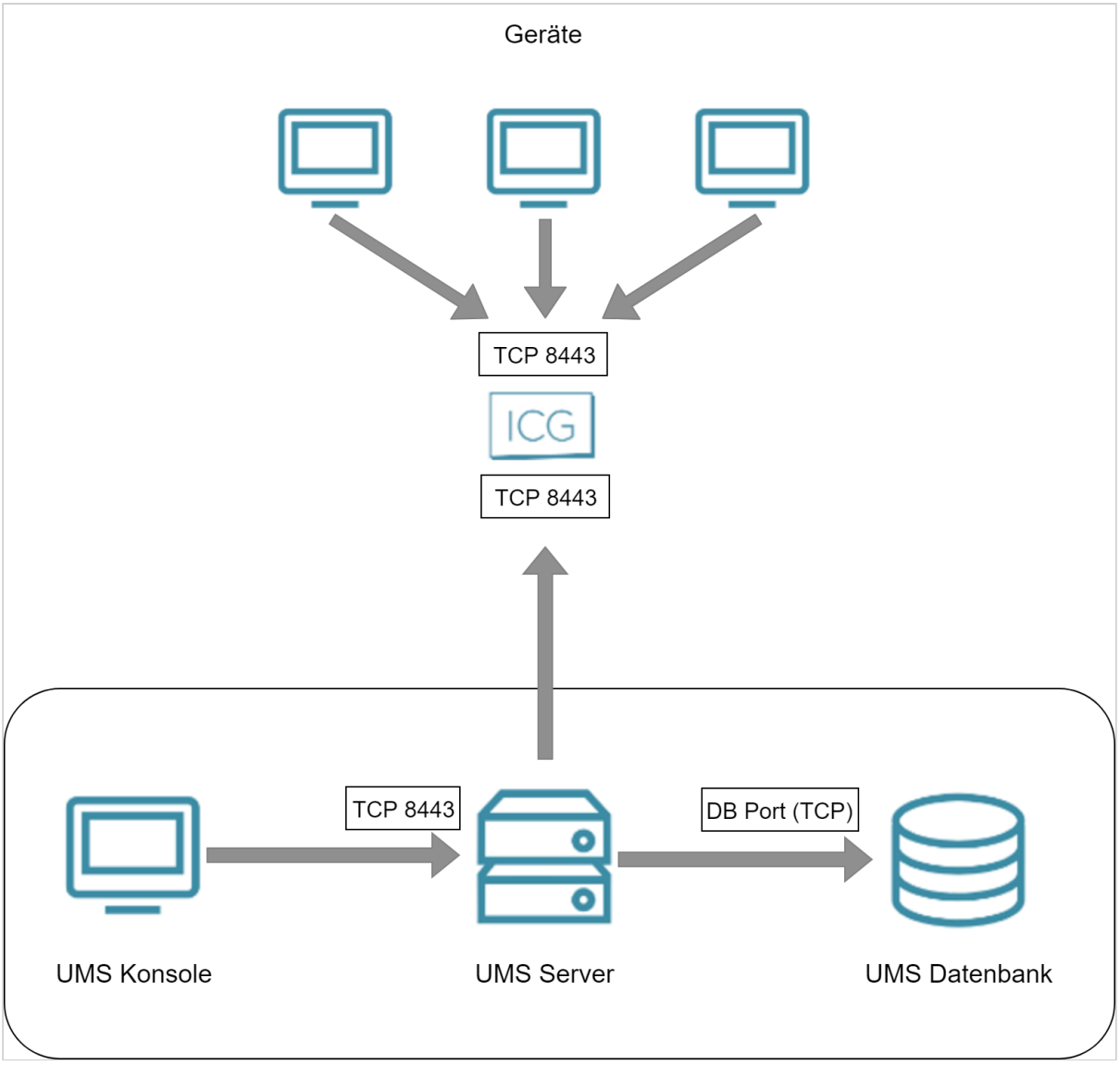
Zur Kommunikation mit den Geräten initiiert die UMS eine TCP-Verbindung zum ICG.

Der Standard-Port, auf dem das ICG lauscht, ist Port 8443. Der Port kann bei der Installation des ICG geändert werden. Ab ICG 2.02 kann ein privilegierter Port verwendet werden, z. B. Port 443. Wenn die Installation abgeschlossen ist, steht der Port fest.

> Mit ICG Version 2.x oder 12.01.x und UMS Version 6.x oder 12.01.x ist es nicht möglich, den TLS-Verkehr zwischen den Komponenten zu untersuchen. Die Inspektion würde TLS brechen und die Kommunikation zwischen den Produkten unterbrechen.
> Ab UMS Version 12.02 können Sie den TLS-Verkehr untersuchen, siehe IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading.

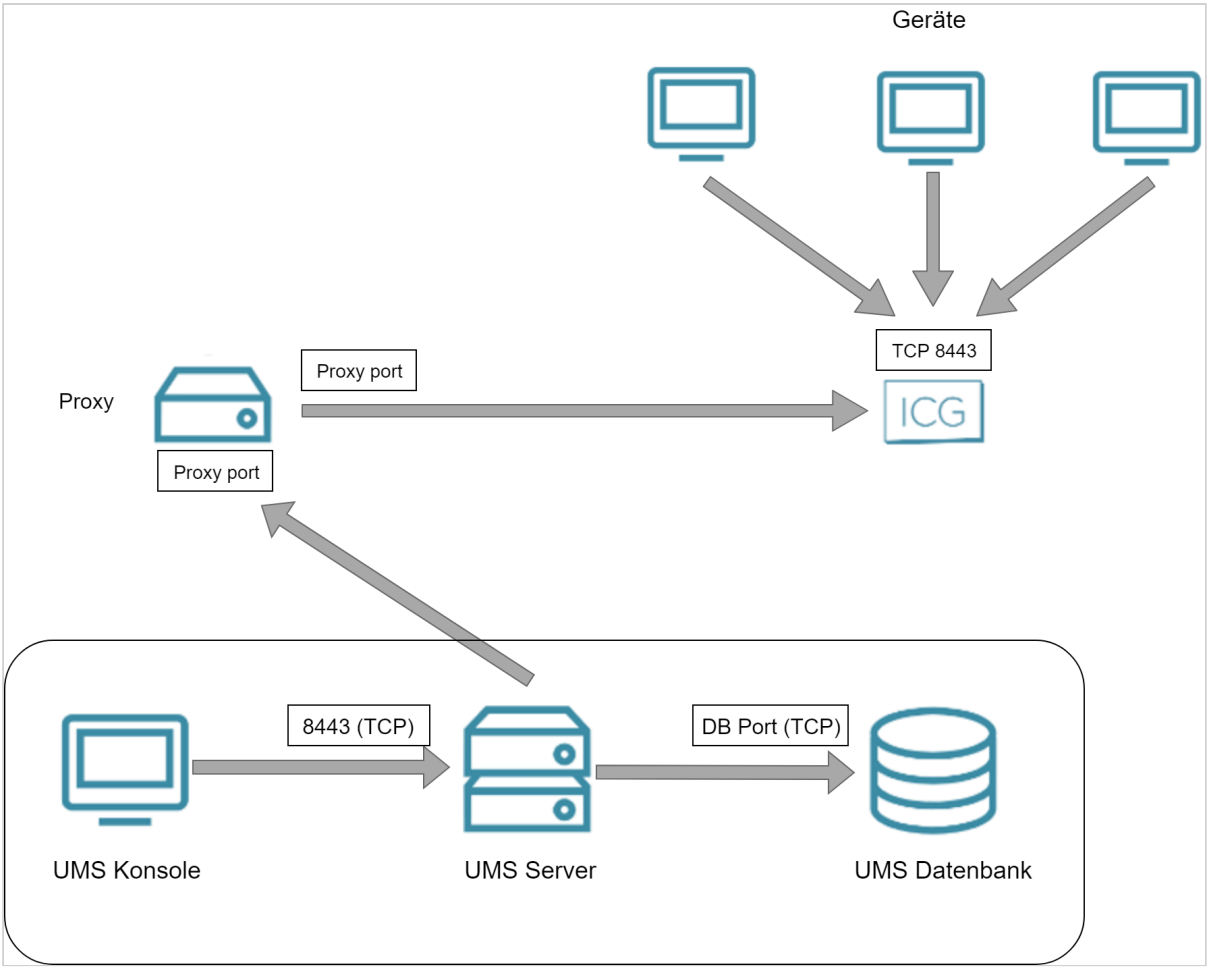
Direkte Verbindung

Die folgende Abbildung veranschaulicht die Kommunikation zwischen den Geräten und der UMS über ICG:



Über Proxy

Die folgende Abbildung veranschaulicht die Kommunikation zwischen den Geräten und der UMS über ICG und einen Proxy:

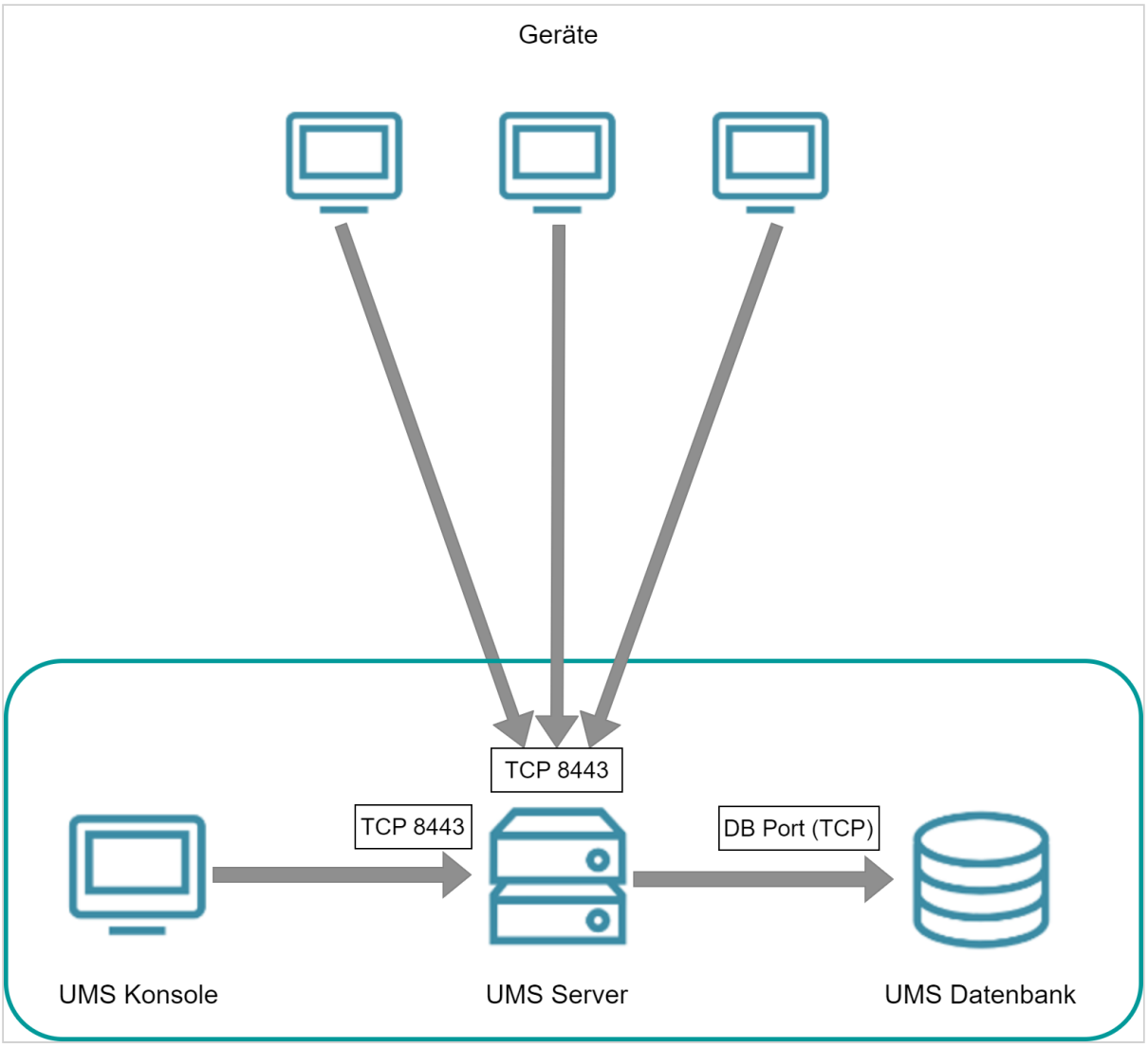

Geräte
TCP 8443
ICG
Proxy
Proxy port
Proxy port
8443 (TCP)
DB Port (TCP)
UMS Konsole
UMS Server
UMS Datenbank

Geräte kontaktieren die UMS

Die folgenden Abbildungen veranschaulichen die Kommunikation zwischen den Geräten und der UMS.

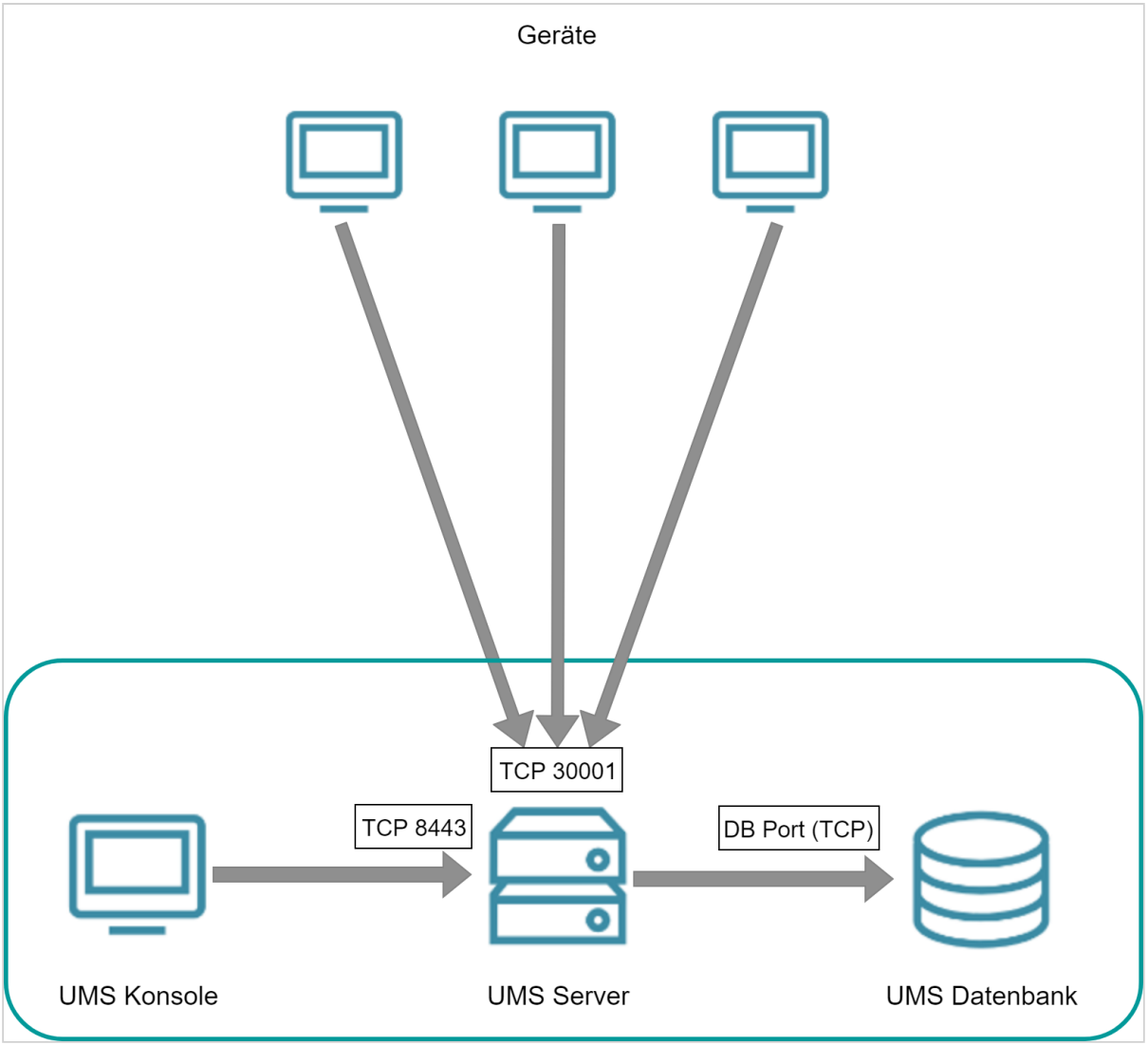
IGEL OS 12

Um mit der UMS zu kommunizieren, initiieren die Geräte über Port 8443 eine TCP-Verbindung zum UMS Server.



IGEL OS 11 oder früher

Um mit der UMS zu kommunizieren, initiieren die Geräte über Port 30001 eine TCP-Verbindung zum UMS Server.


Geräte
TCP 30001
TCP 8443
DB Port (TCP)
UMS Konsole
UMS Server
UMS Datenbank

UMS kontaktiert die Geräte

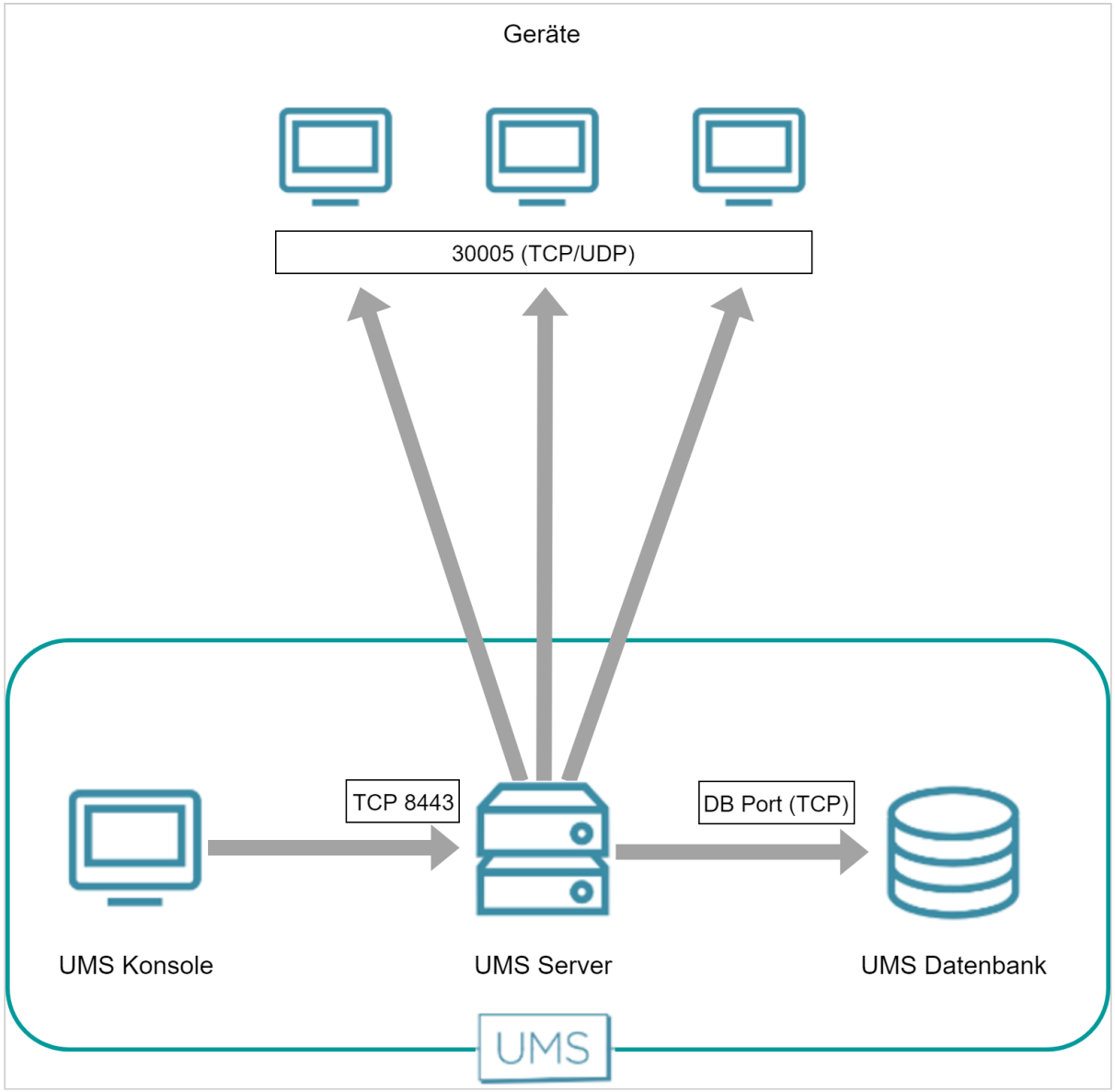
IGEL OS 12

Bei IGEL OS 12-Geräten wird kein zusätzlicher Kanal geöffnet. Es wird ein vorhandener WebSocket (TCP 8443) verwendet.

IGEL OS 11 oder früher

Zur Kommunikation mit IGEL OS 11 Geräten initiiert die UMS über Port 30005 eine TCP-Verbindung zum UMS Agenten des Gerätes.

Die folgende Abbildung veranschaulicht die Kommunikation zwischen der UMS und den Geräten:


Geräte
30005 (TCP/UDP)
TCP 8443
DB Port (TCP)
UMS Konsole
UMS Server
UMS Datenbank
UMS

UMS und Geräte: Spiegeln

IGEL OS 12

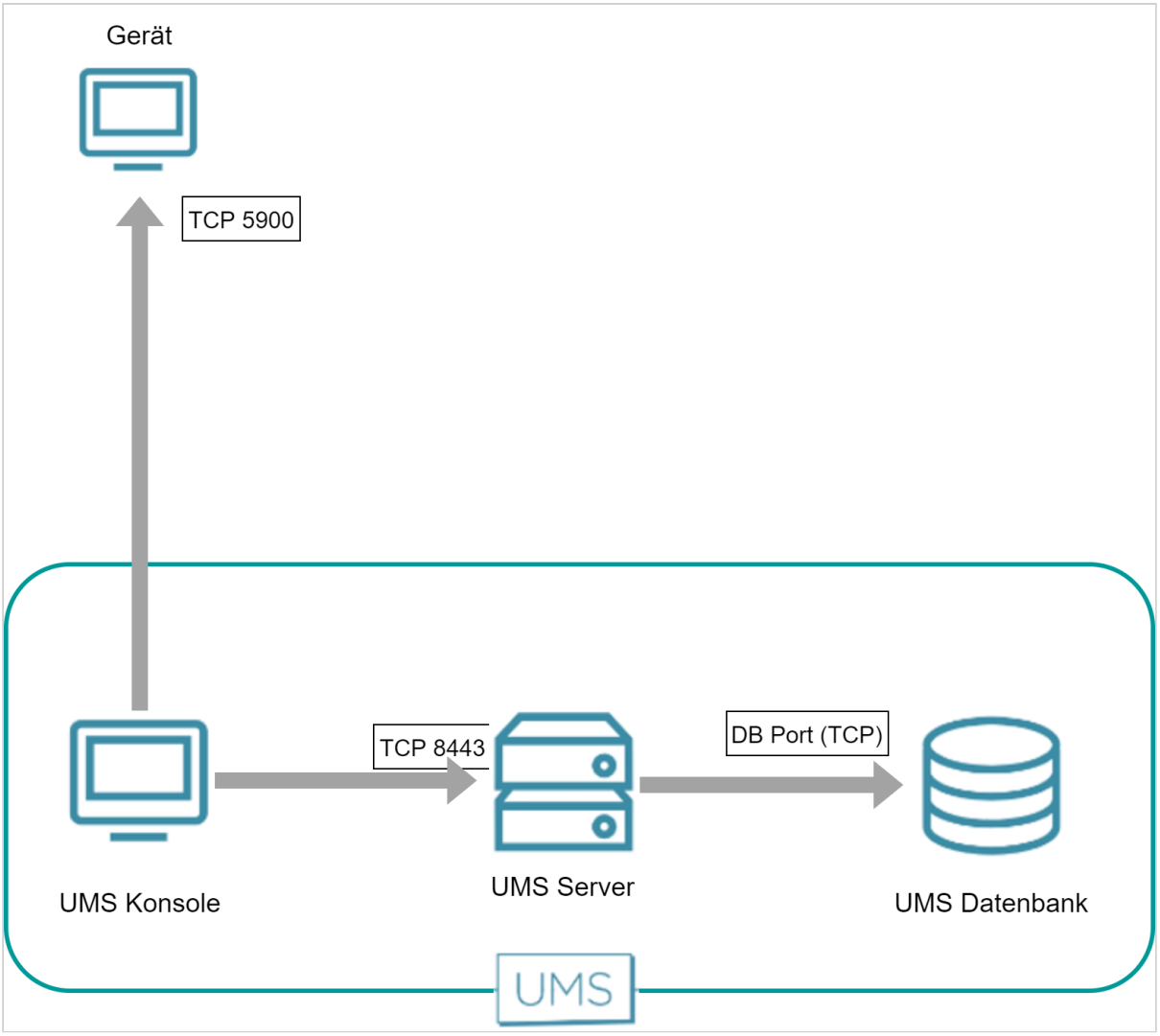
Das Spiegeln von IGEL OS 12-Geräten erfolgt immer sicher, d.h. über das Unified Protocol. Die Kommunikation ist immer verschlüsselt. Siehe UMS und Geräte: Sicheres Spiegeln (see page 39).

IGEL OS 11 oder früher

UMS Konsole

Die UMS Konsole startet eine VNC-Sitzung mit dem Gerät. Der Standard-Port ist 5900 (TCP); der Port kann pro Sitzung geändert werden.

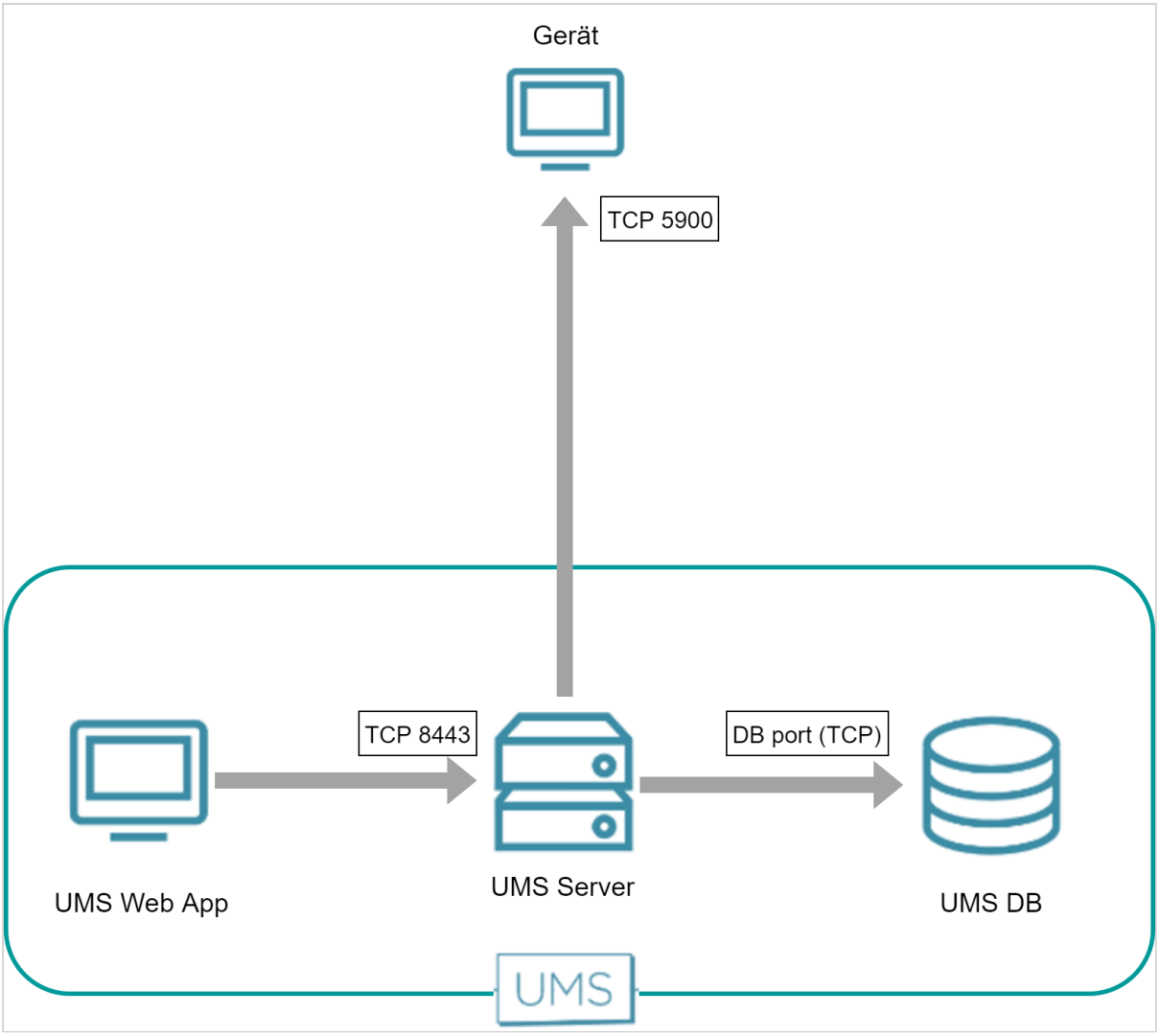
Die folgende Abbildung veranschaulicht die Kommunikation zwischen der UMS Konsole und einem Gerät:



UMS Web App

Die UMS Web App veranlasst den UMS Server, eine VNC-Sitzung für das Spiegeln zu starten. Die VNC-Sitzung wird durch den UMS Server geleitet. Der Standardport für die Kommunikation zwischen dem UMS Server und den Geräten ist 5900 (TCP).

Die folgende Abbildung veranschaulicht die Kommunikation wischen UMS Web App, UMS Server und einem Gerät:


Gerät
TCP 5900
TCP 8443
DB port (TCP)
UMS Web App
UMS Server
UMS DB
UMS

UMS und Geräte: Sicheres Spiegeln

Die folgenden Abbildungen veranschaulichen die Kommunikation zwischen der UMS Konsole / UMS Web App, dem VNC-Viewer, dem UMS Server und dem Gerät.

IGEL OS 12

Das Spiegeln von IGEL OS 12 Geräten erfolgt immer sicher, d.h. über das Unified Protocol. Die Kommunikation ist immer verschlüsselt.

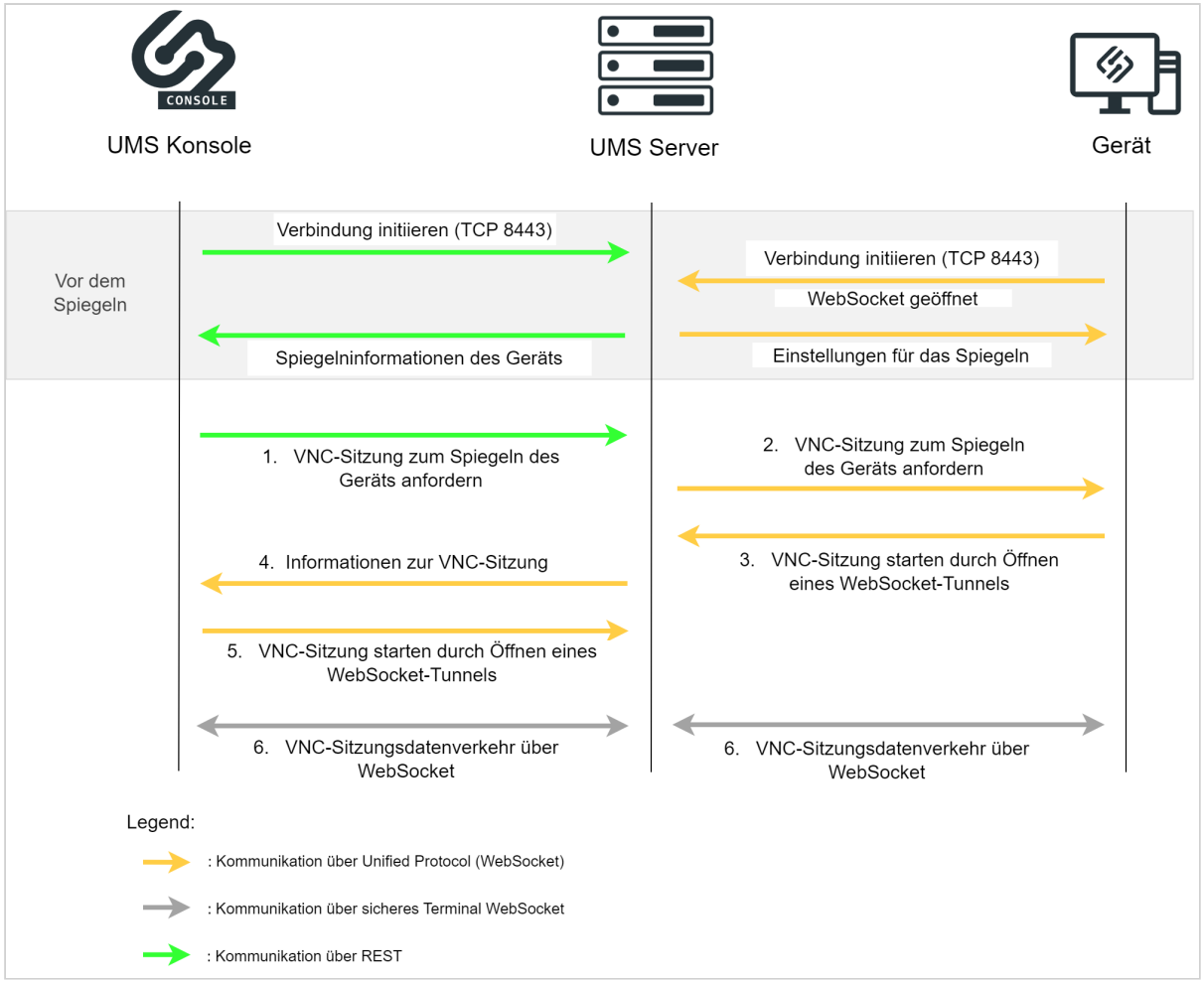
Direkte Verbindung - UMS Konsole (Interner / Externer VNC-Viewer)

Vor dem Spiegeln:

- REST-Verbindung wird zwischen der Konsole und dem UMS-Server hergestellt
- Unified-Protocol-WebSocket-Verbindungen werden initiiert
- Einstellungen und Informationen für das Spiegeln werden weitergeleitet

Spiegeln Kommunikation:

1. Die UMS Konsole fordert den UMS Server auf, eine VNC-Sitzung für das Spiegeln zu initiieren.
2. Der UMS Server fordert das Gerät auf, eine VNC-Sitzung für das Spiegeln zu öffnen.
3. Das Gerät öffnet den WebSocket-Tunnel für das Spiegeln zum UMS Server und startet die VNC-Sitzung.
4. Der UMS Server leitet die VNC-Sitzungsinformationen an die UMS Konsole weiter.
5. Die UMS Konsole öffnet den WebSocket-Tunnel für das Spiegeln und startet die VNC-Sitzung.
6. Die VNC-Daten werden über die geöffneten WebSocket-Tunnel gesendet.



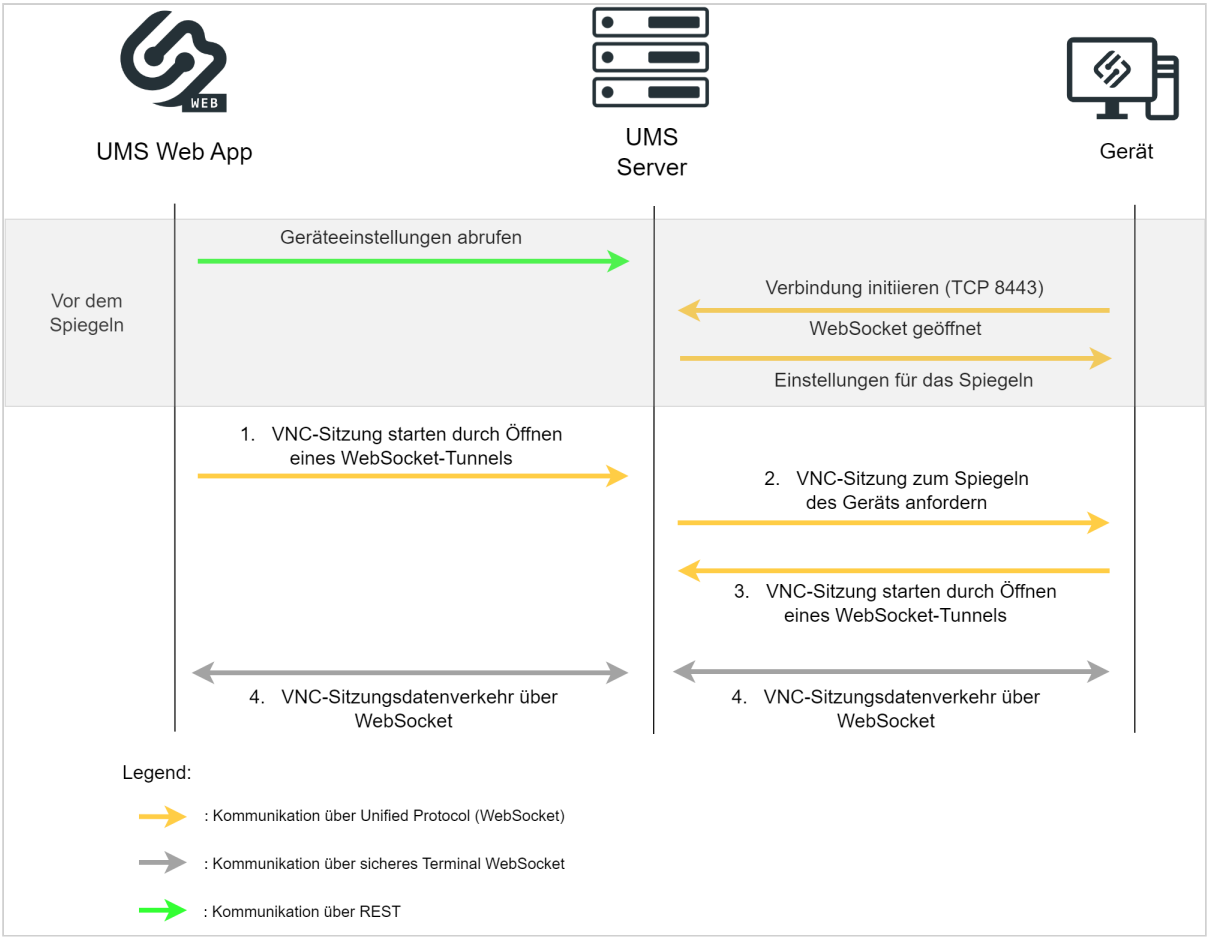
Direkte Verbindung - UMS Web App

Vor dem Spiegeln:

- Geräteeinstellungen werden über REST an den UMS Server gesendet
- Unified-Protocol-WebSocket-Verbindungen werden initiiert zwischen dem Gerät und dem UMS Server
- Einstellungen für das Spiegeln werden weitergeleitet

Spiegeln Kommunikation:

1. Die UMS Web App startet die VNC-Sitzung, indem sie den WebSocket-Tunnel für das Spiegeln zum UMS Server mit Informationen über das zu beschattende Gerät öffnet.
2. Der UMS Server fordert das Gerät über den Unified Protocol WebSocket auf, eine VNC-Sitzung für das Spiegeln zu öffnen.
3. Das Gerät öffnet den WebSocket-Tunnel für das Spiegeln zum UMS Server und startet die VNC-Sitzung.
4. Die VNC-Daten werden über die geöffneten WebSocket-Tunnel gesendet.



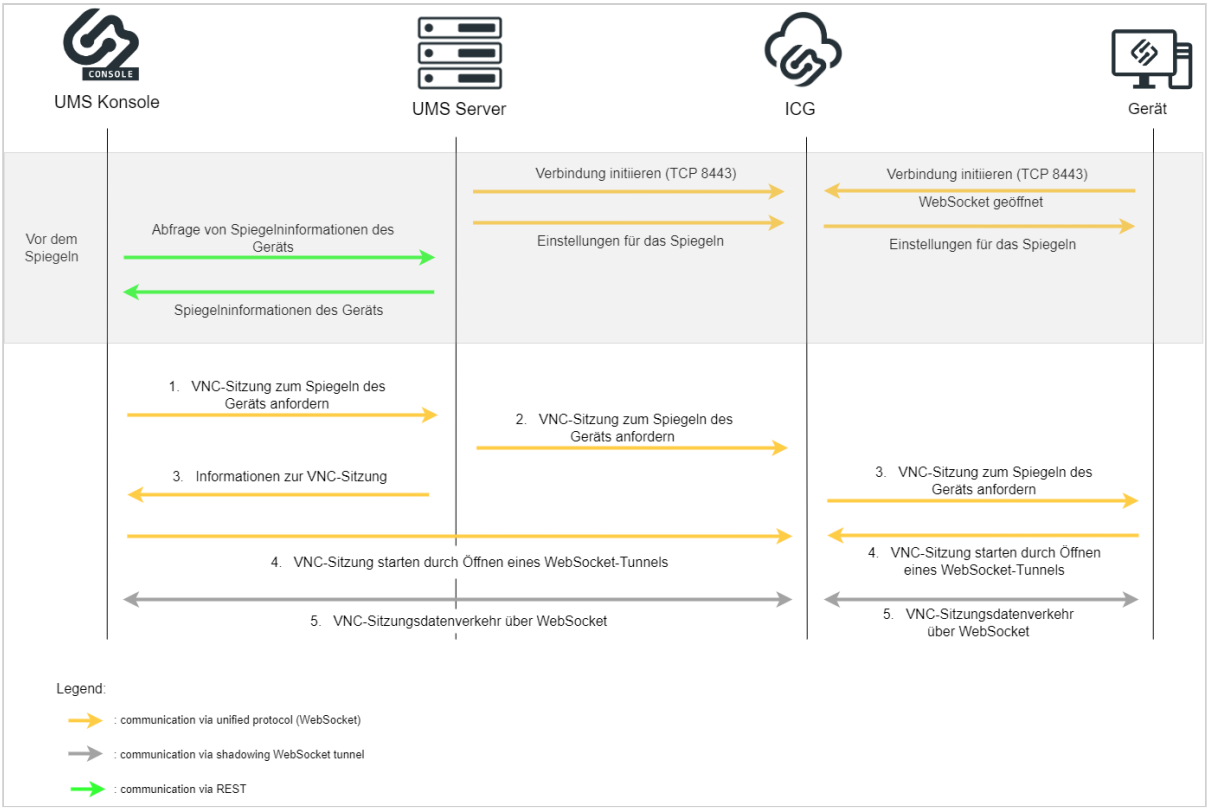
Über ICG - UMS Console (Internal / External VNC Viewer)

Vor dem Spiegeln:

- Unified Protocol WebSocket-Verbindungen werden zwischen dem UMS Server und dem ICG sowie zwischen dem Device und dem ICG initiiert
- Einstellungen und Informationen für das Spiegeln werden weitergeleitet
- UMS Server sendet Shadowing-Informationen über REST an die UMS Konsole

Spiegeln Kommunikation:

1. Die UMS Konsole fordert den UMS Server auf, eine VNC-Sitzung für das Spiegeln zu initiieren.
2. Der UMS Server fordert das ICG auf, eine VNC-Sitzung für das Spiegeln zu öffnen.
3. Der UMS Server sendet die VNC-Informationen an die UMS Konsole und das ICG fordert das Gerät auf, eine VNC-Sitzung für das Spiegeln zu öffnen.
4. Das Gerät öffnet den WebSocket-Tunnel für das Spiegeln zum ICG und startet die VNC-Sitzung und die UMS Konsole öffnet den WebSocket-Tunnel für das Spiegeln zum ICG und startet die VNC-Sitzung.
5. Die VNC-Daten werden über die geöffneten WebSocket-Tunnel gesendet.



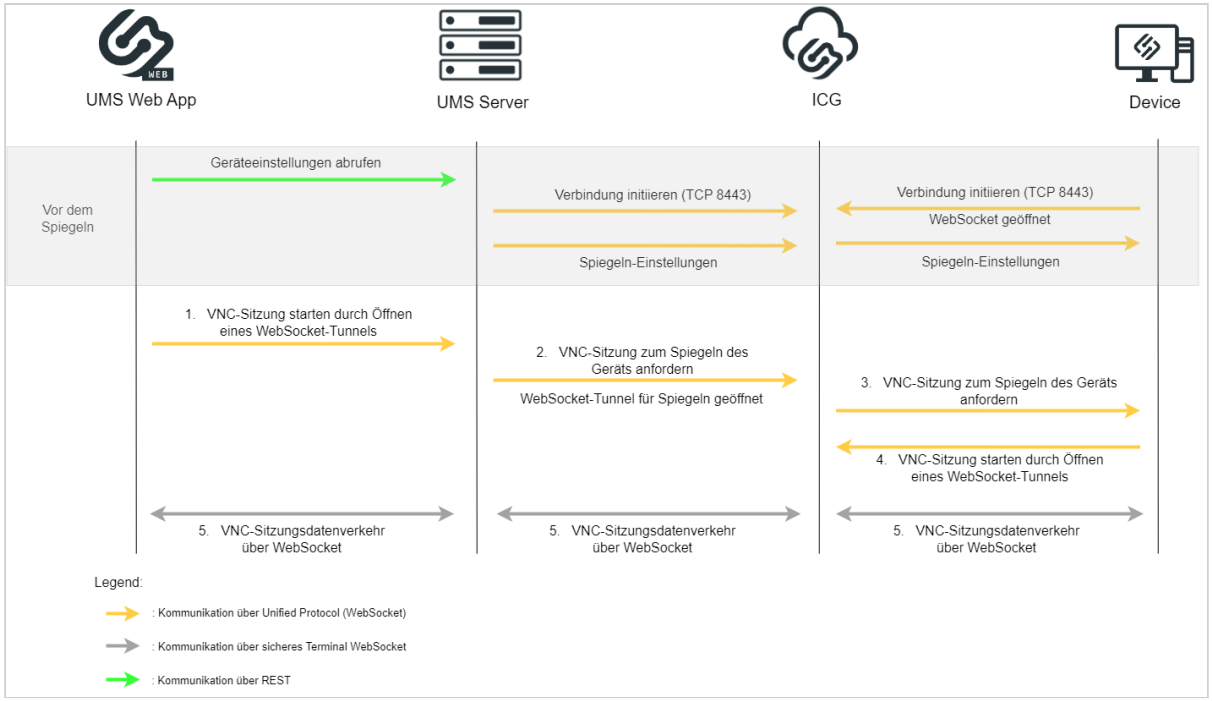
Über ICG - UMS Web App

Vor dem Spiegeln:

- Geräteeinstellungen werden über REST an den UMS Server gesendet
- Unified-Protocol-WebSocket-Verbindungen werden initiiert zwischen dem UMS Server und dem ICG und zwischen dem Gerät und dem UMS Server
- Einstellungen für das Spiegeln werden weitergeleitet

Spiegeln Kommunikation:

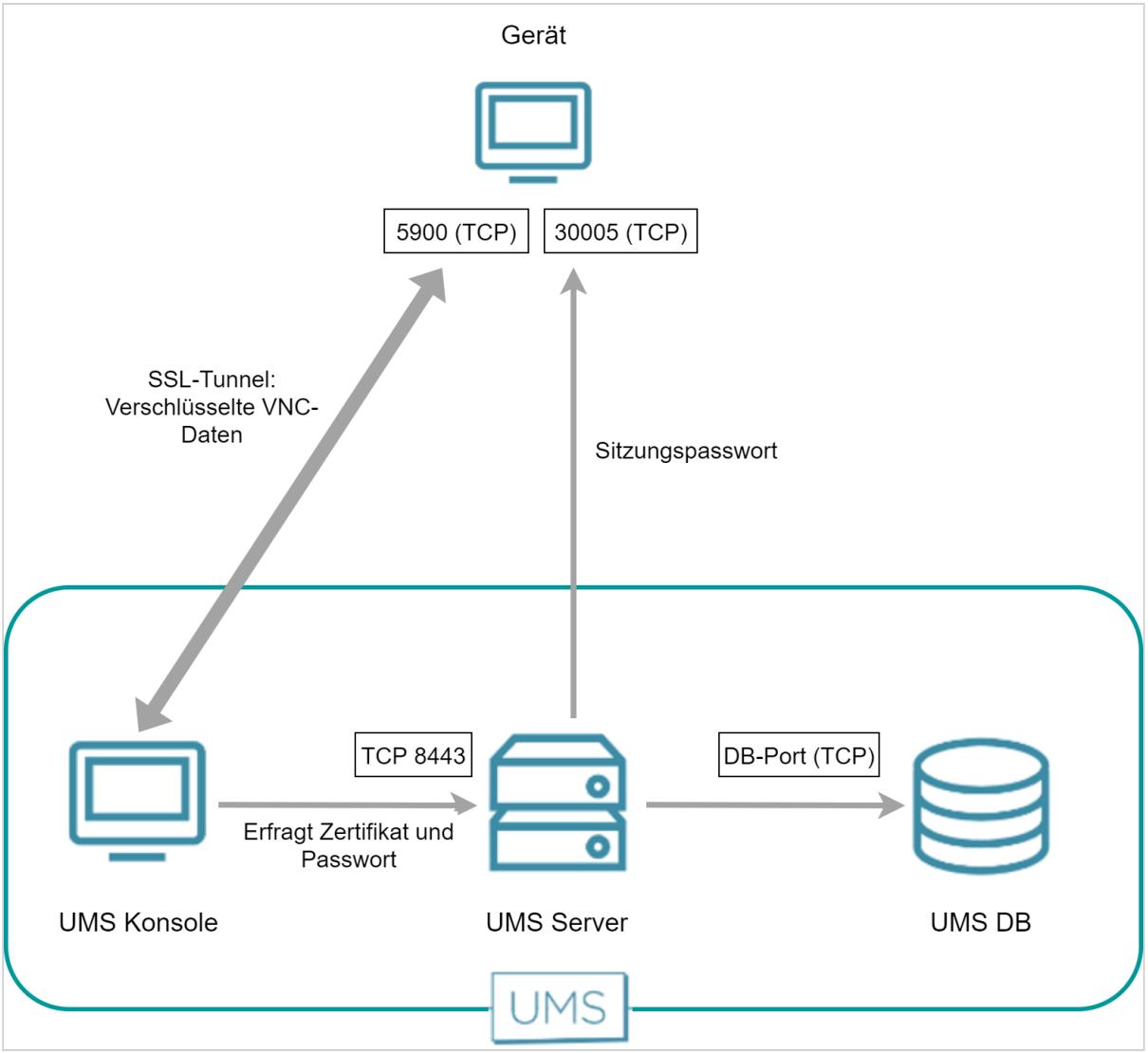
1. Die UMS Web App startet die VNC-Sitzung durch Öffnen des WebSocket-Tunnels für das Spiegeln zum UMS Server mit Informationen über das zu spiegelende Gerät.
2. Der UMS Server fordert das ICG auf, eine VNC-Sitzung für das Spiegeln zu öffnen und öffnet einen WebSocket-Tunnel für das Spiegeln.
3. Das ICG fordert das Gerät auf, eine VNC-Sitzung für das Spiegeln zu öffnen.
4. Das Gerät öffnet den WebSocket-Tunnel für das Spiegeln zum ICG und startet die VNC-Sitzung.
5. Die VNC-Daten werden über diese WebSockets gesendet.



IGEL OS 11 oder früher

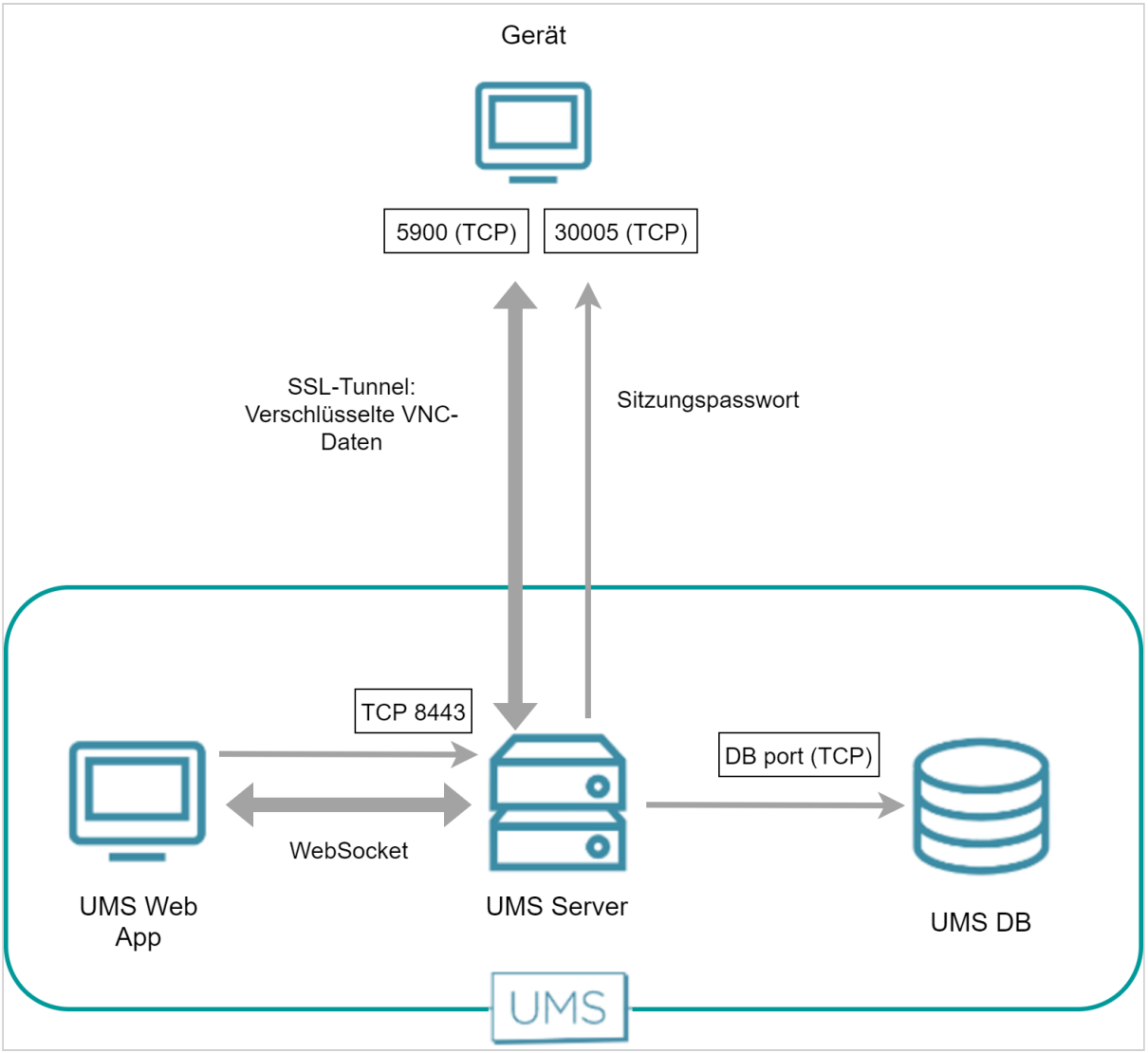
Direkte Verbindung - Interner VNC-Viewer

Die UMS Konsole fragt das Gerätezertifikat und das Sitzungspasswort vom UMS Server ab. Sodann baut die UMS Konsole einen SSL-Tunnel zum Gerät auf, wobei sie das Sitzungspasswort verwendet. Das Gerät sendet das Zertifikat an die UMS Konsole; die UMS Konsole prüft das Zertifikat gegen das Zertifikat, das sie vom UMS Server erhalten hat. Im Gegenzug sendet die UMS Konsole das Sitzungspasswort zum Gerät. Hiernach ist der SSL-Tunnel zwischen UMS Konsole und Gerät aufgebaut und kann zum Austausch von VNC-Daten benutzt werden.



Direkte Verbindung - UMS Web App

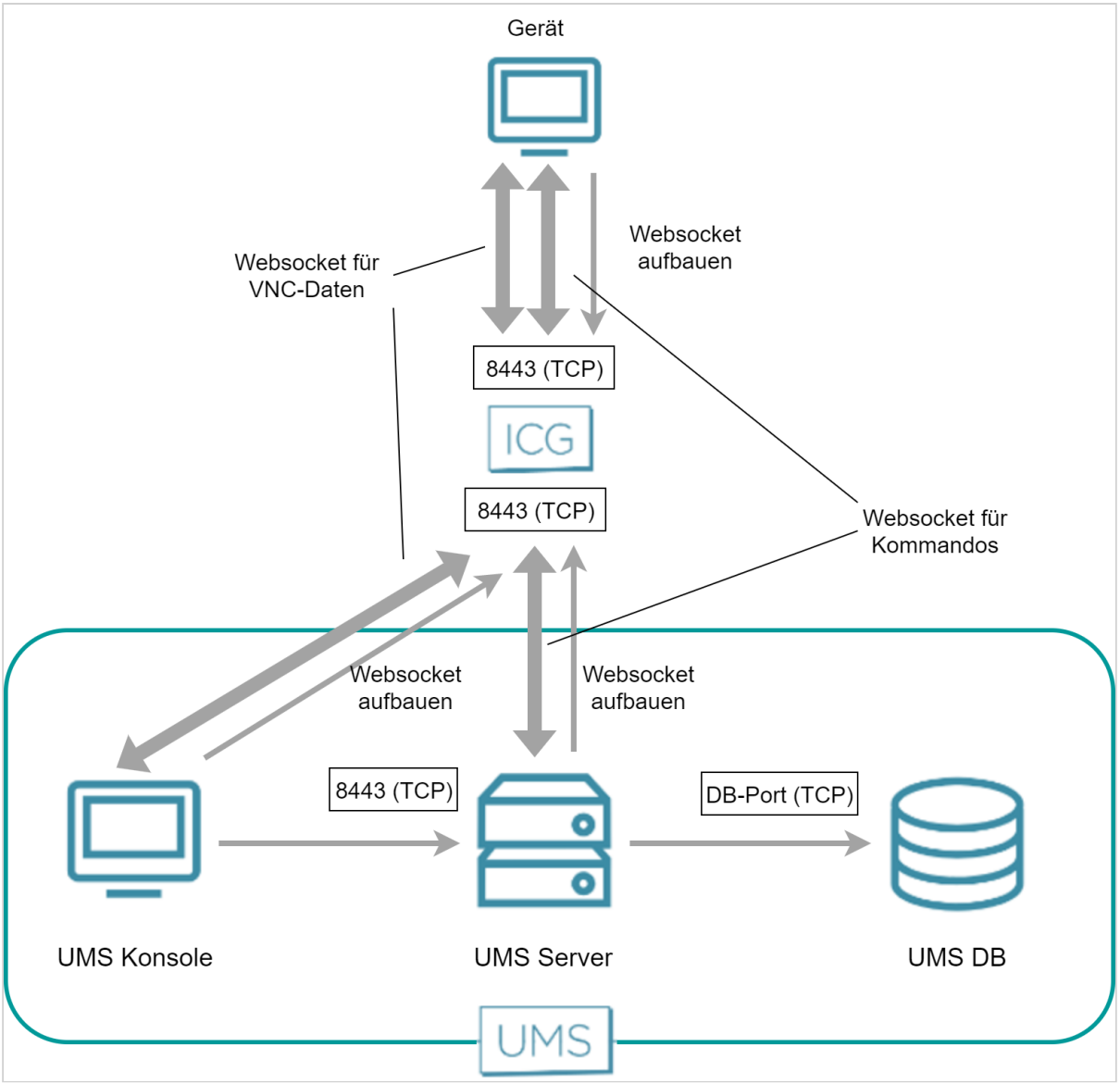
Die UMS Web App veranlasst den UMS Server, eine VNC-Sitzung für das Spiegeln zu initiieren. Der UMS Server baut unter Verwendung eines Sitzungspassworts und des Gerätezertifikats einen SSL-Tunnel zum Gerät auf. UMS Web App und UMS Server kommunizieren über eine WebSocket-Verbindung, die auch die VNC-Daten überträgt.



Über ICG - Interner VNC-Viewer

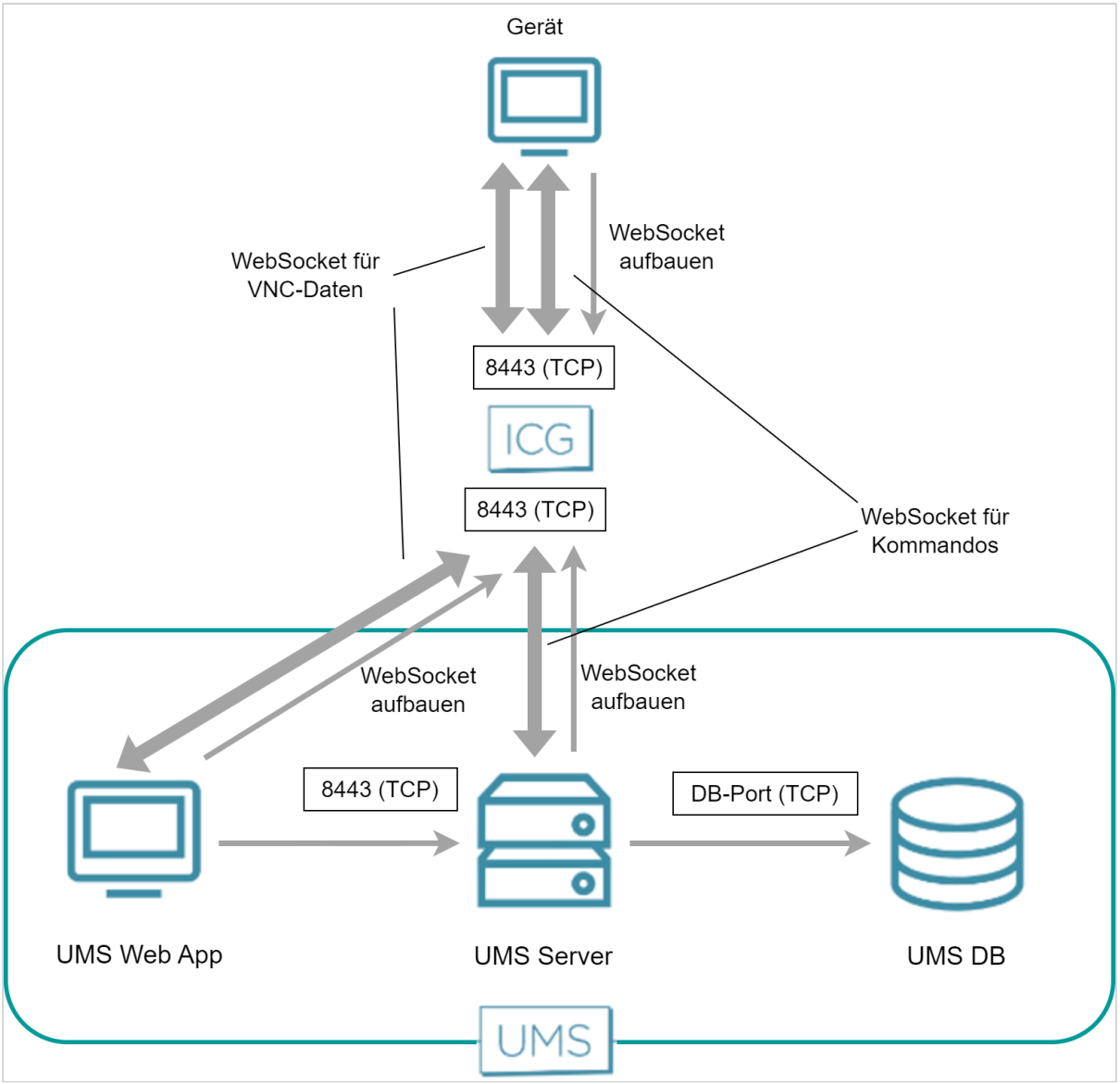
Sowohl der UMS Server als auch das Gerät haben eine Websocket-Verbindung zum ICG aufgebaut; dieser Websocket wird für Kommandos von der UMS und Nachrichten vom Gerät genutzt.

Die UMS Konsole und das Gerät bauen einen dezidierten Websocket für sicheres Spiegeln mit dem ICG auf.



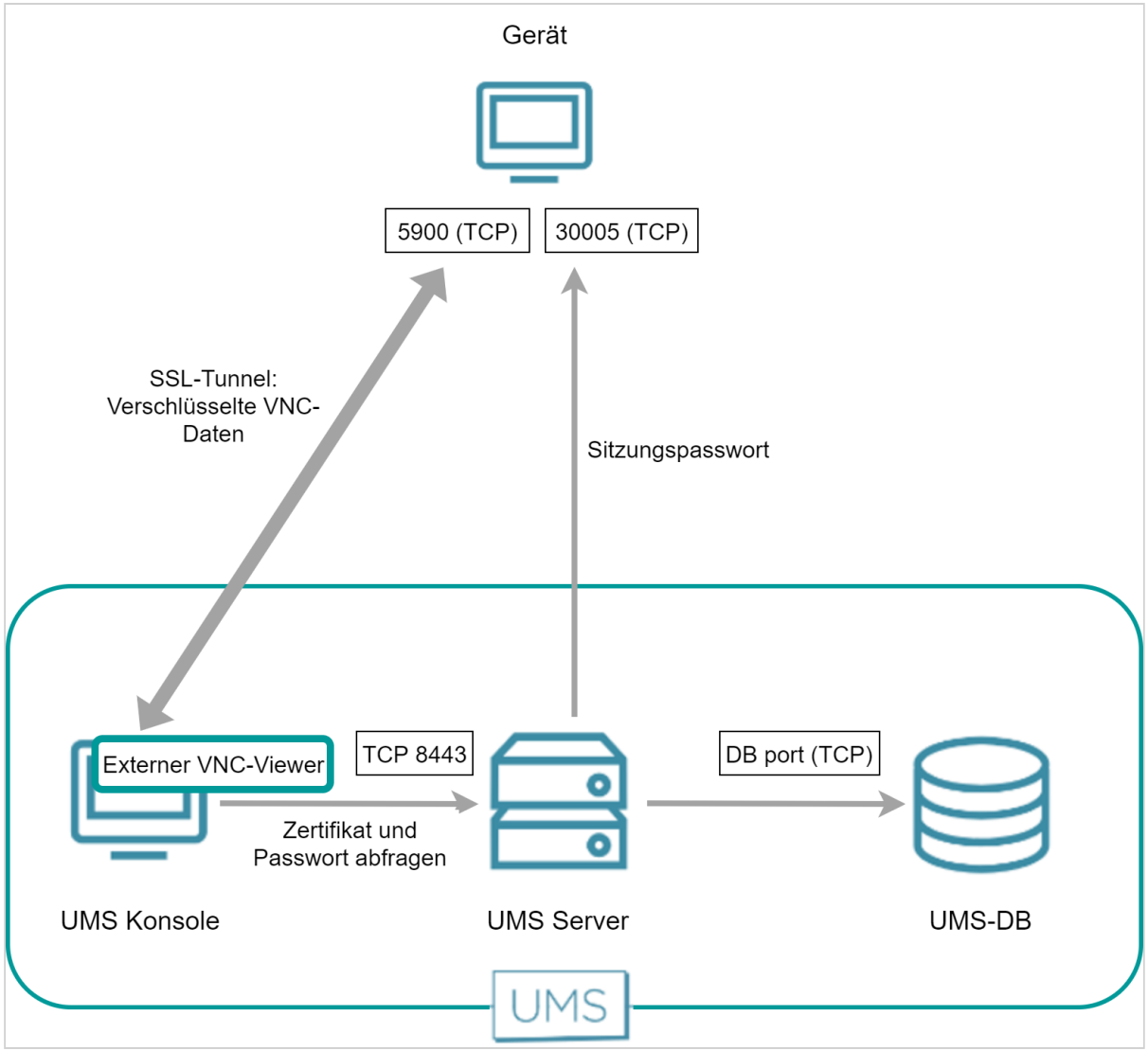
Über ICG - UMS Web App

Die UMS Web App veranlasst den UMS Server, eine VNC-Sitzung für das Spiegeln zu initiieren. Der UMS Server erzeugt eine weitere WebSocket-Verbindung zum Austausch der VNC-Daten. UMS Web App und UMS Server kommunizieren über eine WebSocket-Verbindung, die auch die VNC-Daten überträgt.



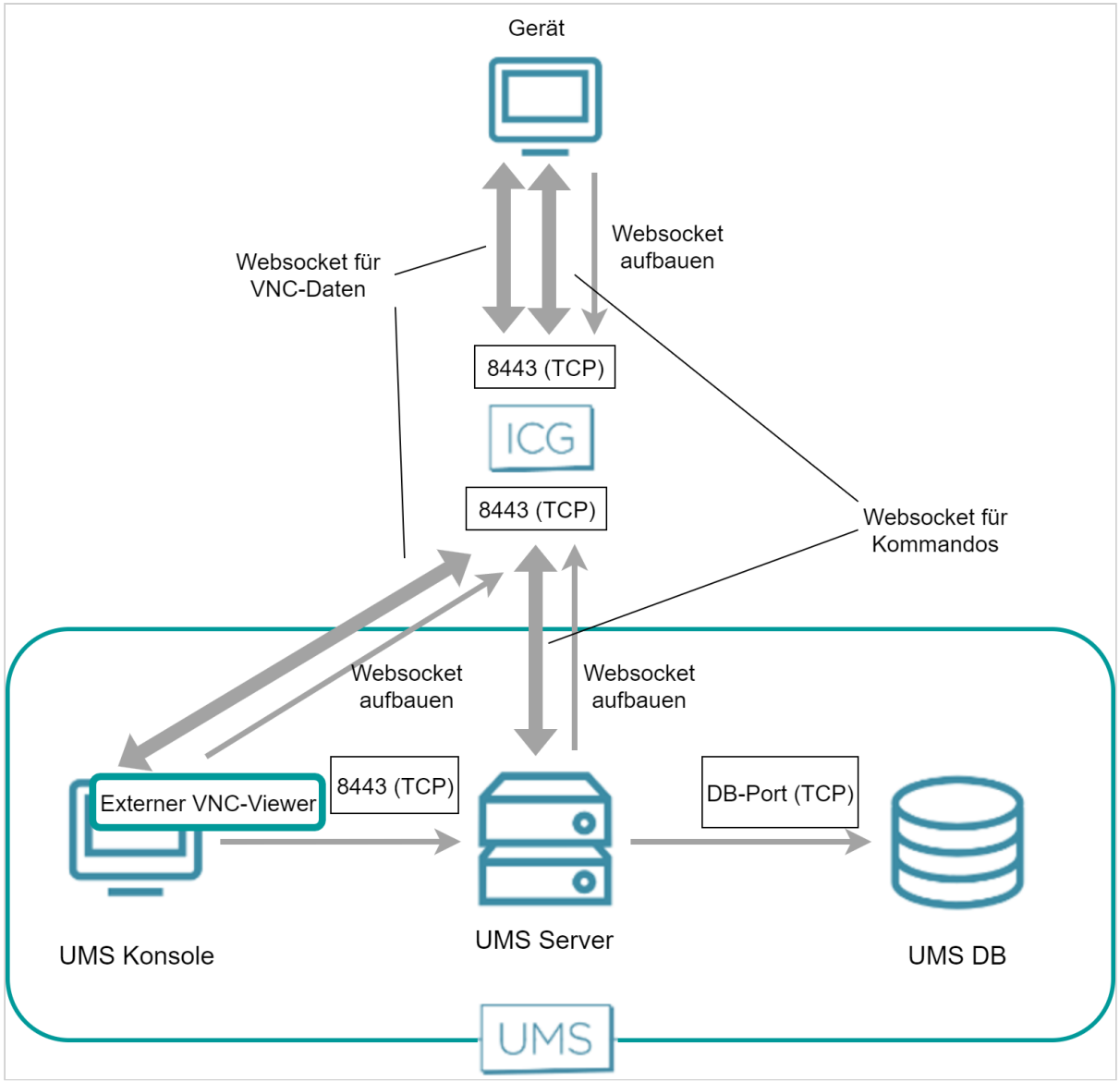
Direkte Verbindung - Externer Viewer

Der externe VNC-Viewer läuft auf der selben Maschine wie die UMS Konsole. Die UMS Konsole startet den externen Viewer und fungiert dann als Proxy zwischen dem Gerät und dem externen Viewer.



Über ICG - Externer VNC-Viewer

Der externe VNC-Viewer läuft auf der selben Maschine wie die UMS Konsole. Die UMS Konsole startet den externen Viewer und fungiert dann als Proxy zwischen dem Gerät und dem externen Viewer.


Gerät
Websocket für
VNC-Daten
Websocket
aufbauen
8443 (TCP)
ICG
8443 (TCP)
Websocket für
Kommandos
Websocket
aufbauen
Websocket
aufbauen
Externer VNC-Viewer
8443 (TCP)
DB-Port (TCP)
UMS Konsole
UMS Server
UMS DB
UMS

UMS und Geräte: Sicheres Terminal

Dieser Artikel beschreibt die Kommunikation einer sicheren Terminalsitzung in der IGEL Universal Management Suite (UMS) Umgebung.

IGEL OS 12

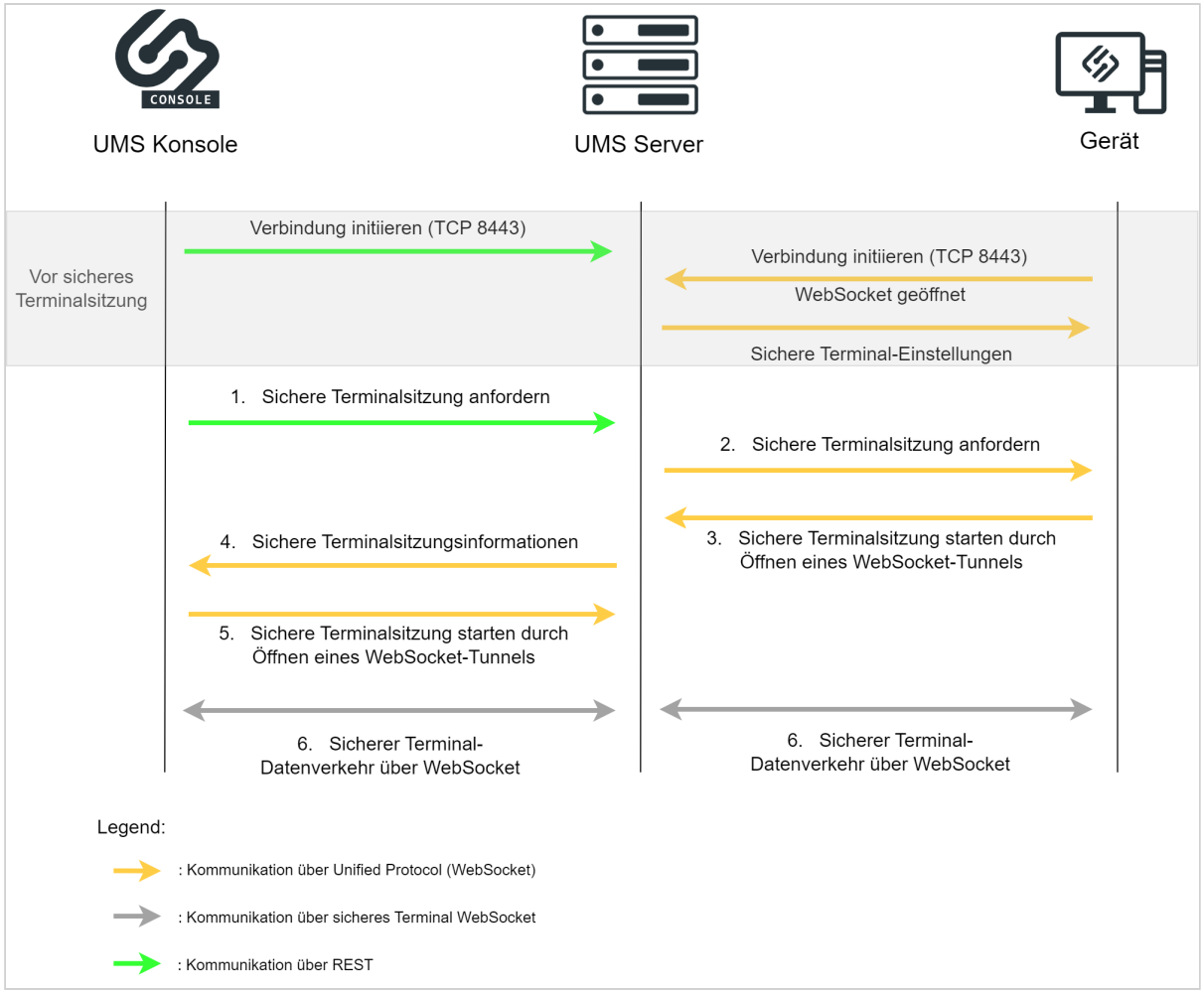
Direkte Verbindung

Vor der sicheren Terminalsitzung:

- REST-Verbindung wird zwischen der Konsole und dem UMS Server initiiert
- Unified Protocol WebSocket-Verbindung wird zwischen dem Gerät und dem UMS Server initiiert
- Sichere Terminaleinstellungen werden weitergeleitet

Sichere Terminal-Kommunikation:

1. Die UMS Konsole fordert den UMS Server auf, eine sichere Terminalsitzung zu initiieren.
2. Der UMS Server fordert das Gerät über den Unified Protocol WebSocket auf, die sichere Terminalsitzung zu öffnen.
3. Das Gerät öffnet den WebSocket-Tunnel für sichere Terminaldaten zum UMS Server und startet die sichere Terminalsitzung.
4. Der UMS Server leitet die Informationen über die sichere Terminalsitzung an die UMS Konsole weiter.
5. Die UMS Konsole öffnet den WebSocket-Tunnel für sichere Terminaldaten zum UMS Server und startet die sichere Terminalsitzung.
6. Die Terminaldaten werden über die geöffneten WebSockets gesendet.



Über ICG

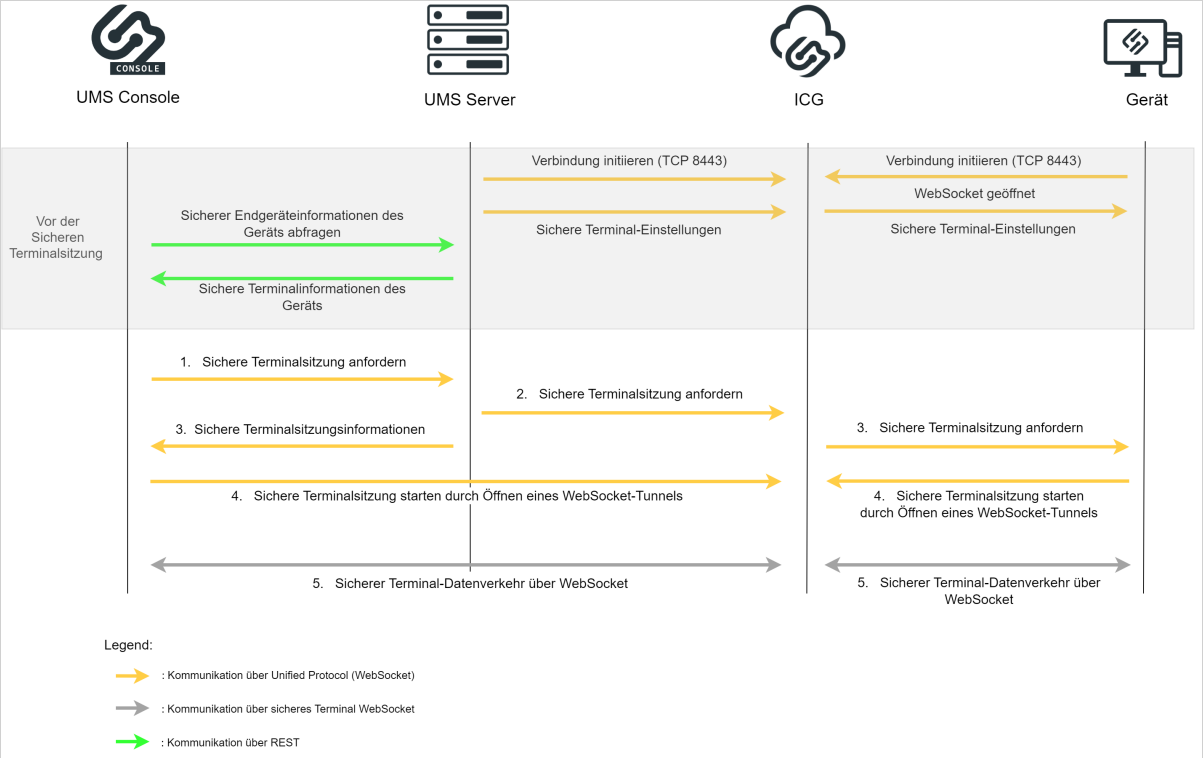
Vor der sicheren Terminalsitzung:

- Unified Protocol WebSocket-Verbindungen werden zwischen dem UMS Server und dem ICG sowie zwischen dem Gerät und dem ICG initiiert
- Sichere Terminaleinstellungen werden weitergeleitet
- UMS Server sendet sichere Terminalinformationen des Geräts über REST an die UMS Konsole

Sichere Terminal-Kommunikation:

1. Die UMS Konsole fordert den UMS Server auf, eine sichere Terminalsitzung zu initiieren.
2. Der UMS Server fordert das ICG auf, eine sichere Terminalsitzung zu eröffnen.
3. Das ICG fordert das Gerät über das Unified Protocol WebSocket auf, eine sichere Terminalsitzung zu eröffnen, und der UMS Server leitet die Informationen zur sicheren Terminalsitzung an die UMS Konsole weiter.
4. Das Gerät öffnet den WebSocket-Tunnel für sichere Terminaldaten zum ICG und startet die sichere Terminalsitzung, und die UMS Konsole öffnet den WebSocket-Tunnel für sichere Terminaldaten zum ICG und startet die sichere Terminalsitzung.

5. Die Terminaldaten werden über die geöffneten WebSockets gesendet.

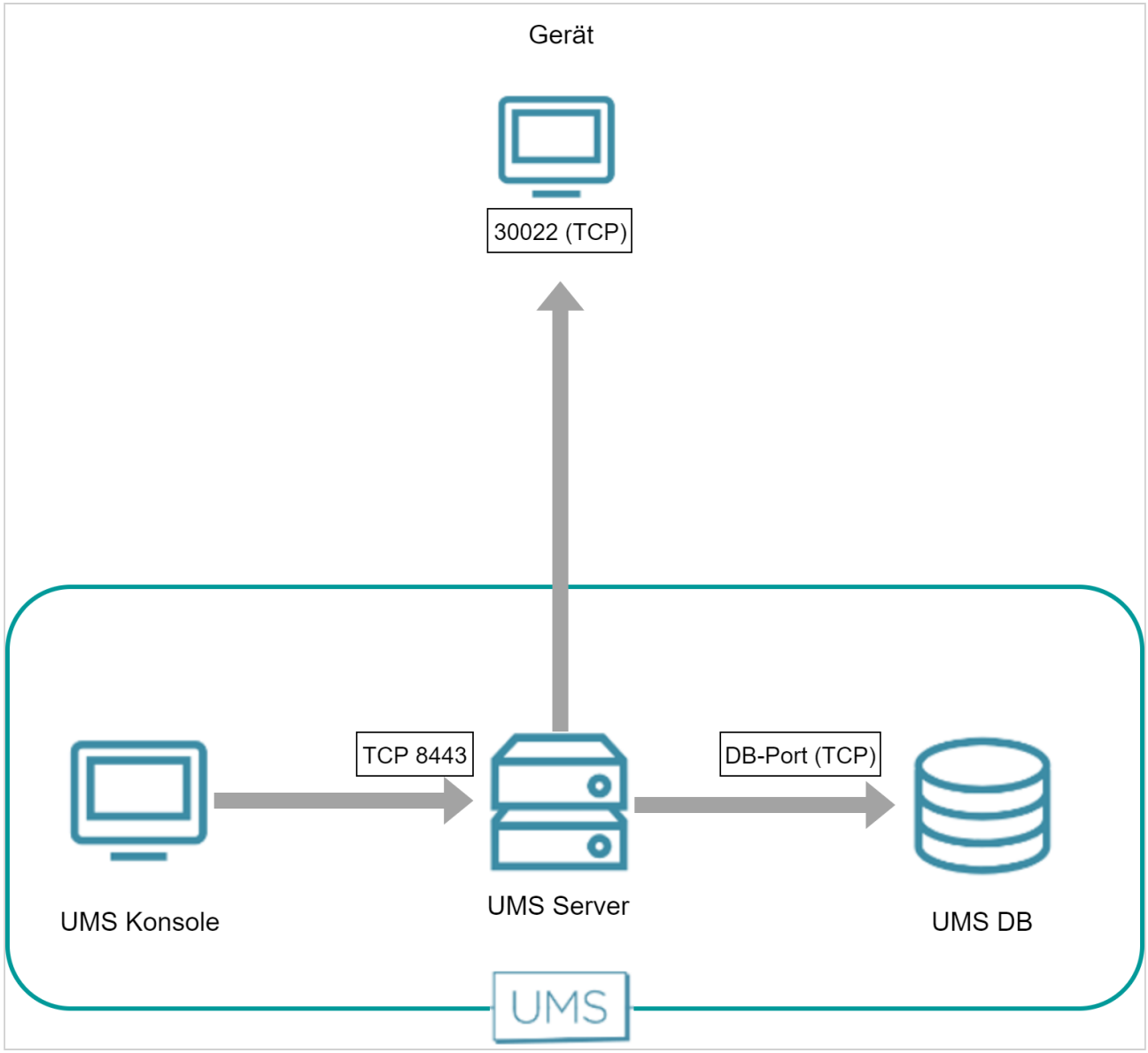


IGEL OS 11 oder früher

Direkte Verbindung

Die UMS Konsole baut eine Verbindung zum UMS Server auf. Daraufhin baut der UMS Server einen TLS-Tunnel zum Gerät auf.

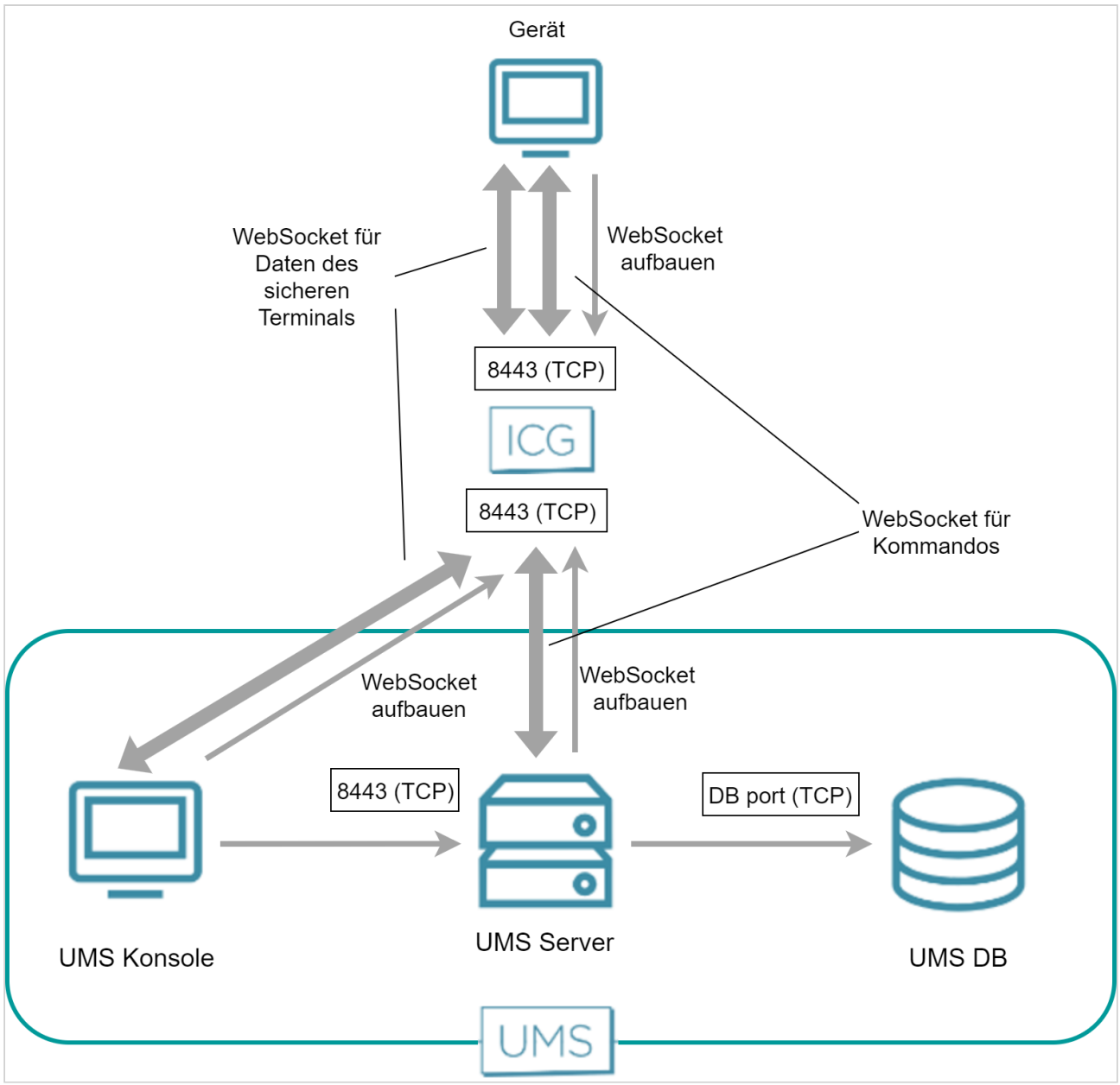
Die folgende Abbildung veranschaulicht die Kommunikation zwischen der UMS Konsole, dem UMS Server und einem Gerät:



Über ICG

Sowohl der UMS Server als auch das Gerät haben eine WebSocket-Verbindung zum ICG aufgebaut; dieser WebSocket wird für Kommandos von der UMS sowie für Nachrichten vom Gerät verwendet.

Die UMS Konsole und das Gerät bauen einen dedizierten WebSocket für das sichere Terminal mit dem ICG auf.


Gerät
WebSocket für Daten des sicheren Terminals
WebSocket aufbauen
8443 (TCP)
ICG
8443 (TCP)
WebSocket für Kommandos
WebSocket aufbauen
WebSocket aufbauen
8443 (TCP)
DB port (TCP)
UMS Konsole
UMS Server
UMS DB
UMS

UMS und Geräte: Dateiübertragung

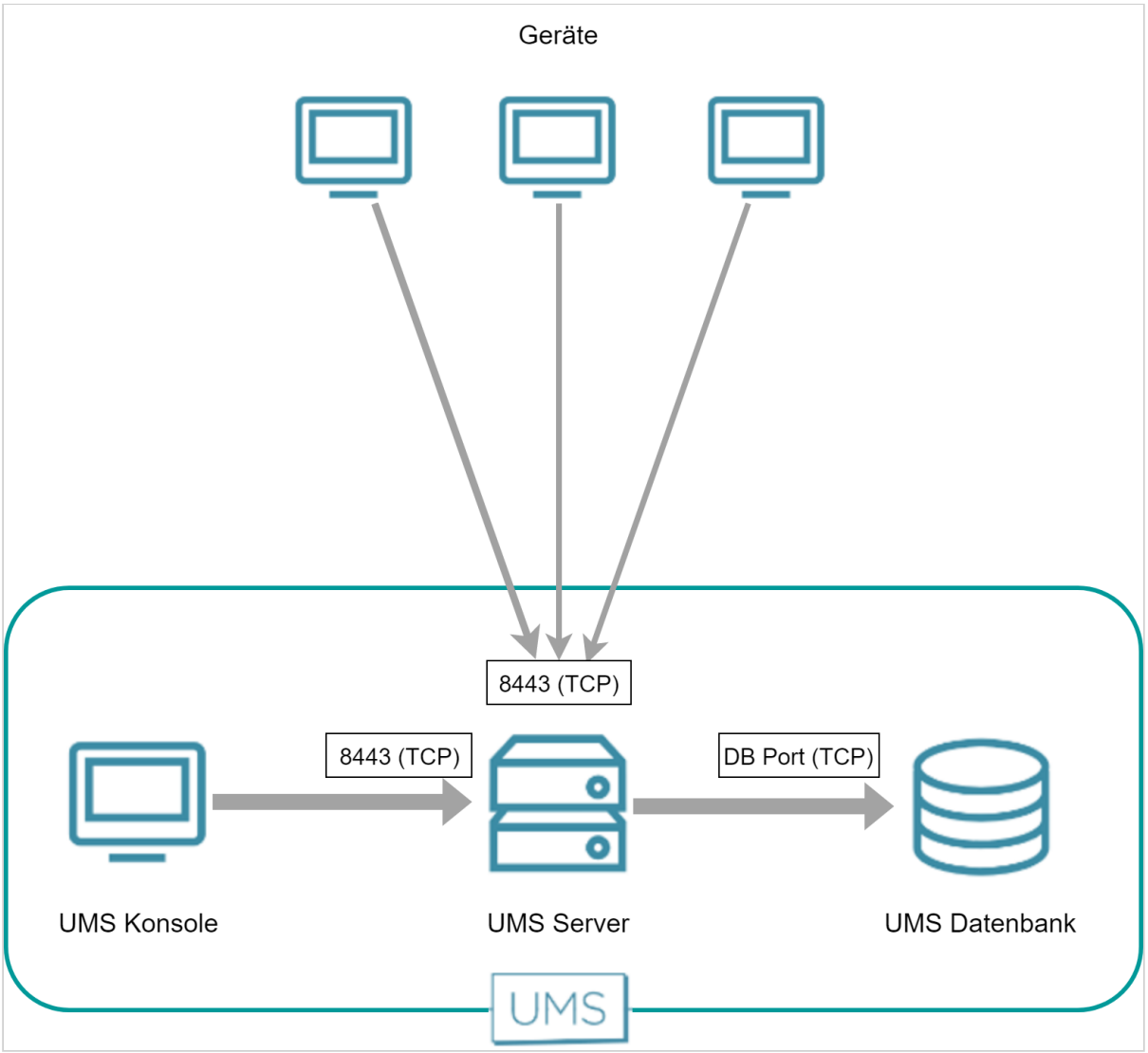
IGEL OS 12

Bei IGEL OS 12-Geräten wird für die Dateiübertragung kein zusätzlicher Kanal geöffnet. Es wird ein vorhandener WebSocket (TCP 8443) verwendet.

IGEL OS 11 oder früher

Um Dateien, z. B. ein Hintergrundbild oder Protokolldateien, aus der UMS zu holen, senden die Geräte eine HTTPS-Anfrage an den UMS Server. Der UMS Server empfängt auf Port 8443.

Die folgende Abbildung veranschaulicht die Kommunikation zwischen den Geräten und der UMS:



Universal Firmware Update

Mit der Funktion Universal Firmware Update kann die UMS nach neuen Firmware-Updates suchen und die gewünschte Firmware in ein WebDAV-Verzeichnis oder einen FTP-Server herunterladen. Die Verbindung zum IGEL-Downloadserver kann direkt oder über einen Proxy erfolgen.

Weitere Informationen zu dieser Funktion finden Sie unter Universal Firmware Update (1) (see page 56) im UMS Handbuch.

> Das Feature Universal Firmware Update ist für Geräte mit IGEL OS 11 und früher relevant, nicht für IGEL OS 12-Geräte.

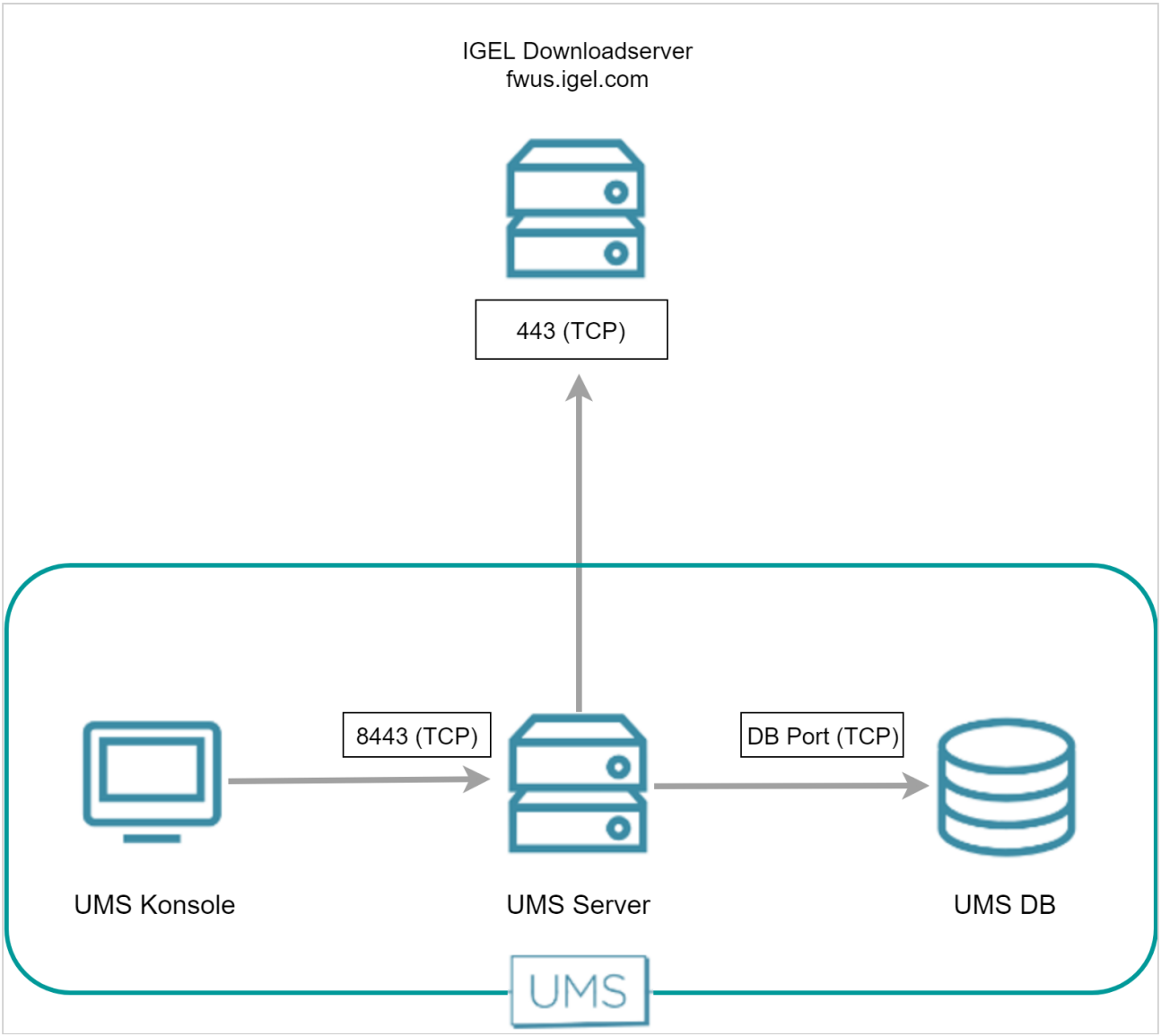
UMS kontaktiert den Downloadserver, um nach neuen Updates zu suchen

> Das Feature Universal Firmware Update ist für Geräte mit IGEL OS 11 und früher relevant, nicht für IGEL OS 12-Geräte.

Die UMS initiiert eine TCP-Verbindung zum Port 443 von fwus.igel.com. Der IGEL Downloadserver sendet eine Antwort mit einer Liste von Downloadlinks, die es der UMS ermöglichen, die gewünschte Firmware herunterzuladen.

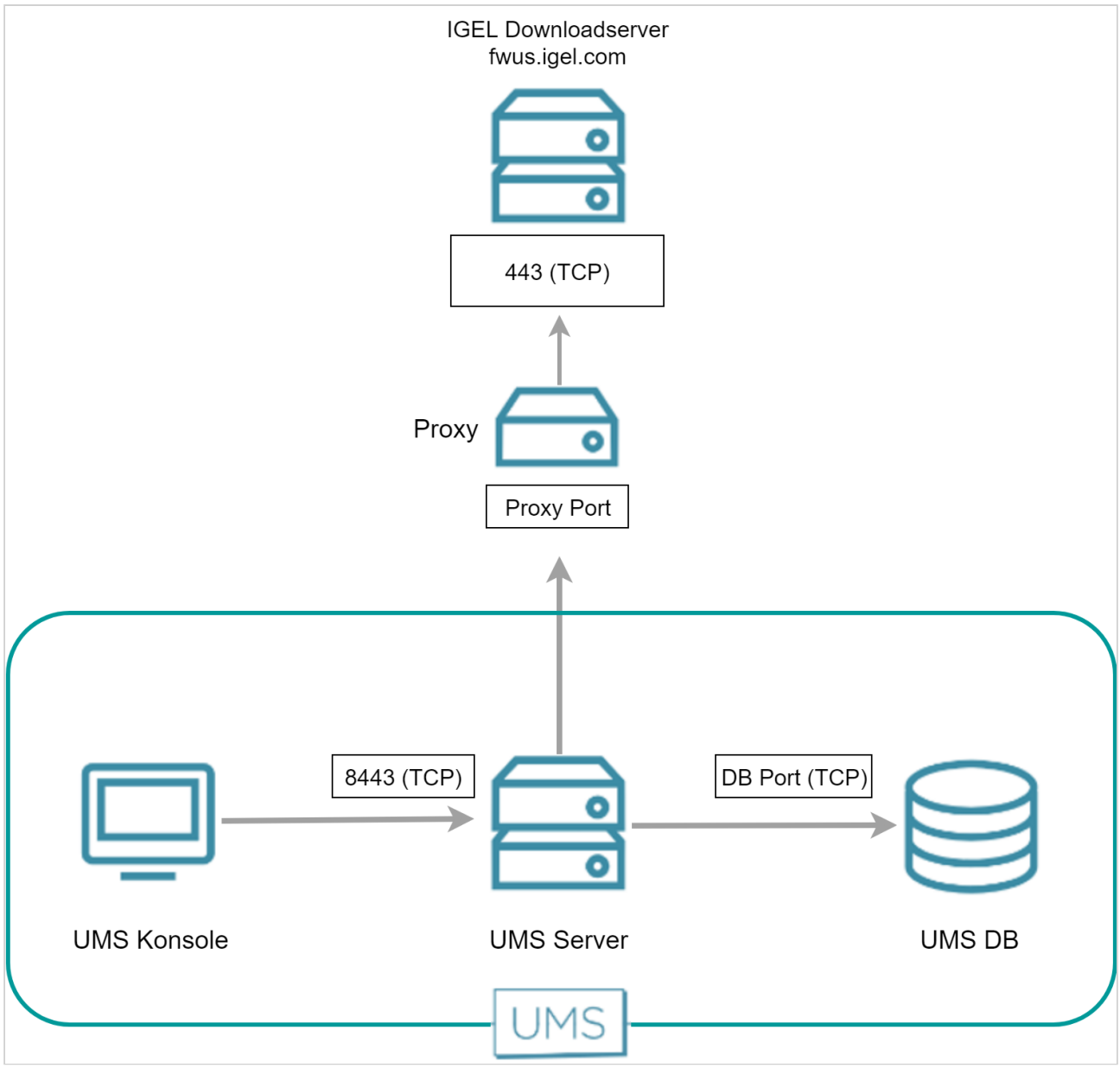
Direkte Verbindung

Die folgende Abbildung veranschaulicht die Kommunikation zwischen dem UMS Server und den IGEL Downloadservern:



Über Proxy

Wenn sich ein Proxy zwischen der UMS und den IGEL Downloadservern befindet, muss der Port, auf dem der Proxy lauscht, unter **UMS Administration > Globale Konfiguration > Proxyserver** angegeben werden.


IGEL Downloadserver
fwus.igel.com
443 (TCP)
Proxy
Proxy Port
8443 (TCP)
DB Port (TCP)
UMS Konsole
UMS Server
UMS DB
UMS

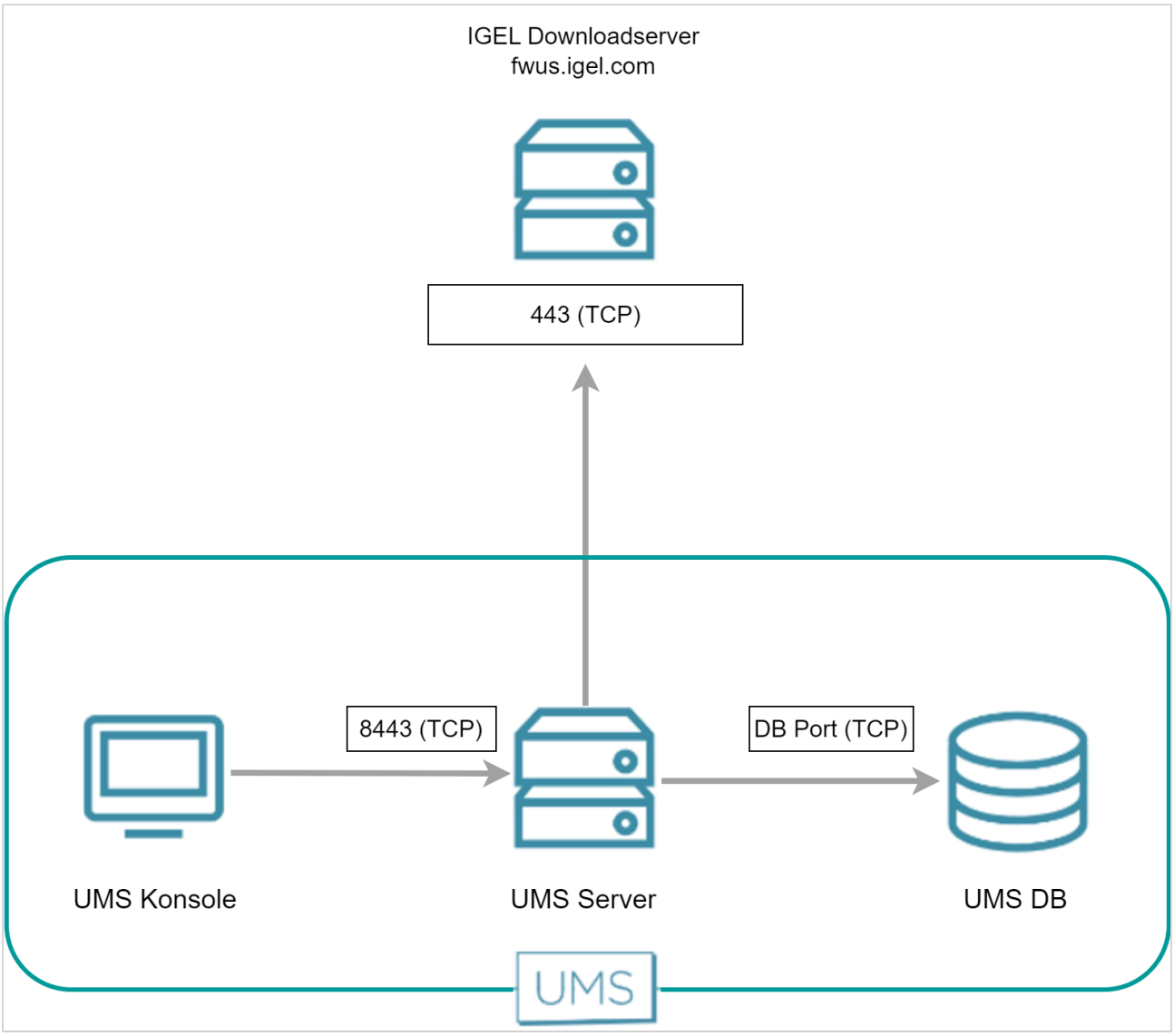
UMS Firmware herunterladen

> Das Feature Universal Firmware Update ist für Geräte mit IGEL OS 11 und früher relevant, nicht für IGEL OS 12-Geräte.

Die UMS lädt die gewünschte Firmware mithilfe der URLs herunter, die es vom Downloadserver erhalten hat. Die UMS verwendet Port 443 für fwus.igel.com.

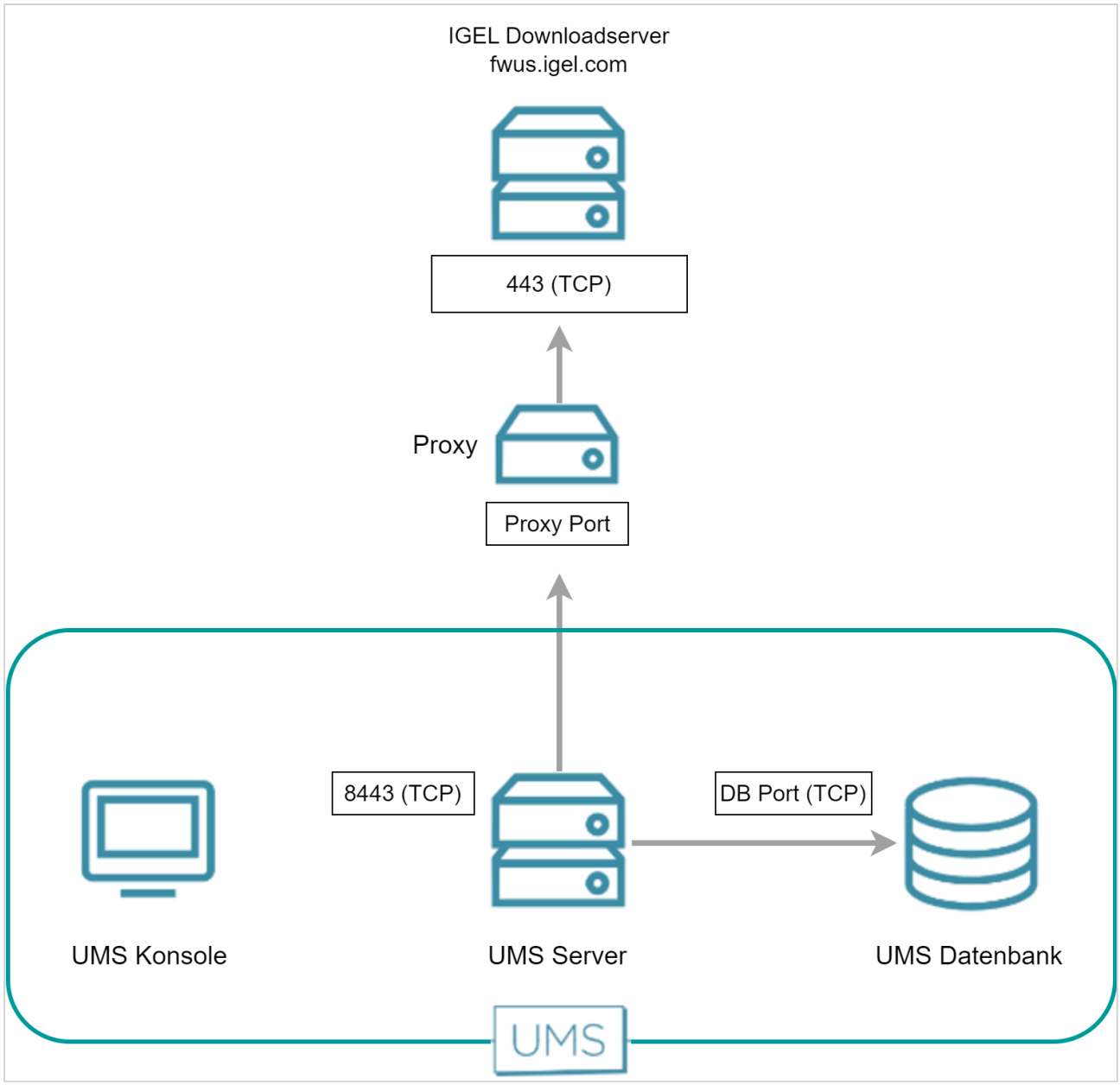
Direkte Verbindung

Die folgende Abbildung veranschaulicht die Kommunikation zwischen dem UMS Server und den IGEL Downloadservern:



Über Proxyserver

Wenn ein Proxyserver zwischen der UMS und dem IGEL Downloadserver platziert wird, muss der Port für den Proxyserver unter **UMS Administration > Globale Konfiguration > Proxyserver** angegeben werden.



Automatic License Deployment (ALD)

Die Funktion Automatic License Deployment (ALD) ist eine Methode zur Bereitstellung von Lizenzen für UD3, UMA und UD Pocket.

Weitere Informationen zu dieser Funktion finden Sie unter How to Set Up and Use Automatic License Deployment (ALD).

Die automatische Lizenzbereitstellung kann über eine Direktverbindung oder über einen Proxy erfolgen.

Die Schritte des Verfahrens werden in den folgenden Abschnitten beschrieben:

- UMS Kontaktaufnahme mit dem Lizenzserver (see page 63)
- UMS sendet neue Einstellungen an die Geräte (see page 65)
- Geräte kontaktieren die UMS, um Lizenzdateien herunterzuladen (see page 66)

UMS Kontaktaufnahme mit dem Lizenzserver

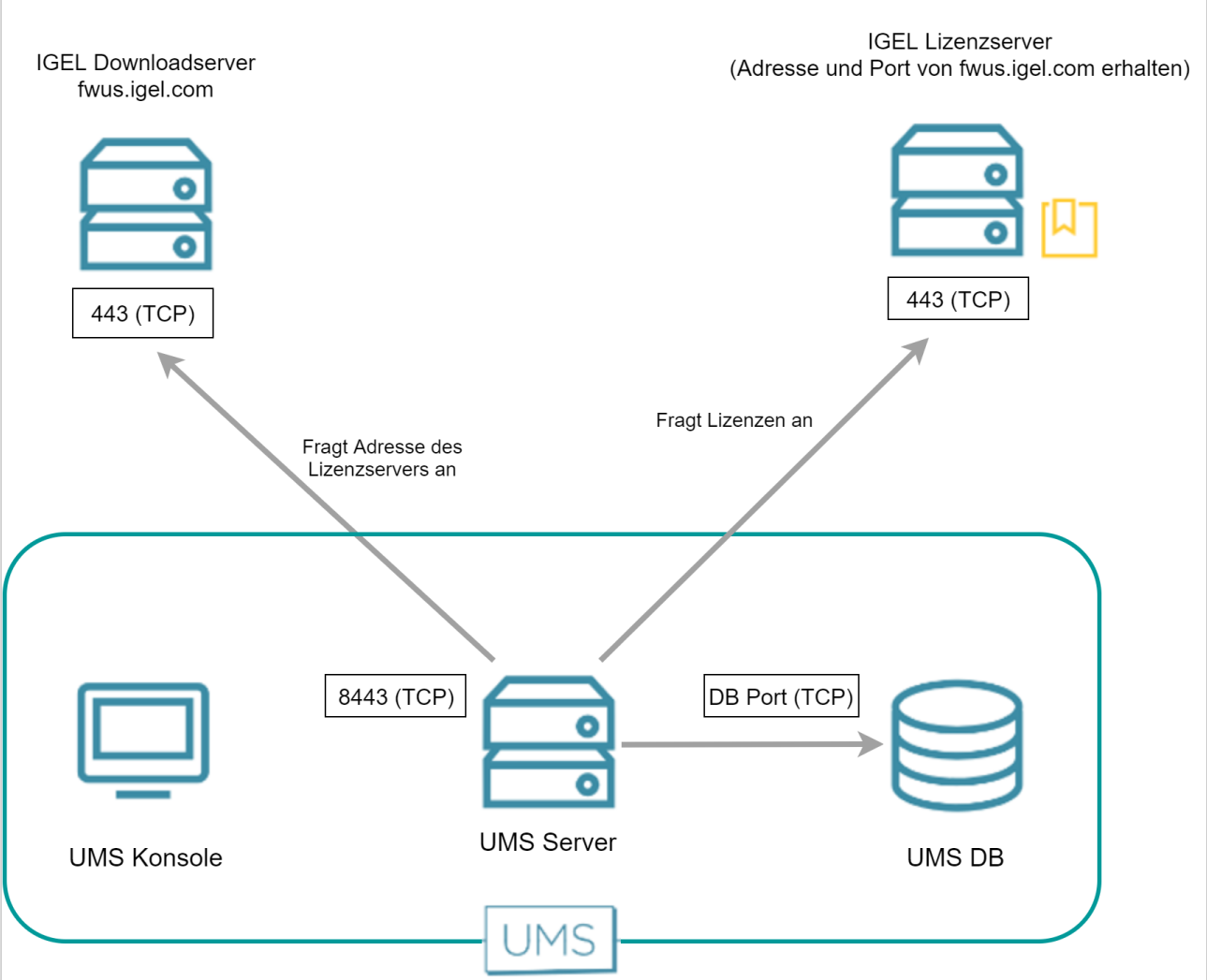
Die UMS erfragt die Verbindungsdaten vom IGEL Downloadserver fwus.igel.com und kontaktiert dann den IGEL Lizenzserver. Derzeit lauten die Verbindungsdetails wie folgt:

- URL: susi.igel.com
- Port: 443

> Die Verbindungsdaten können in Zukunft geändert werden.

Direkte Verbindung

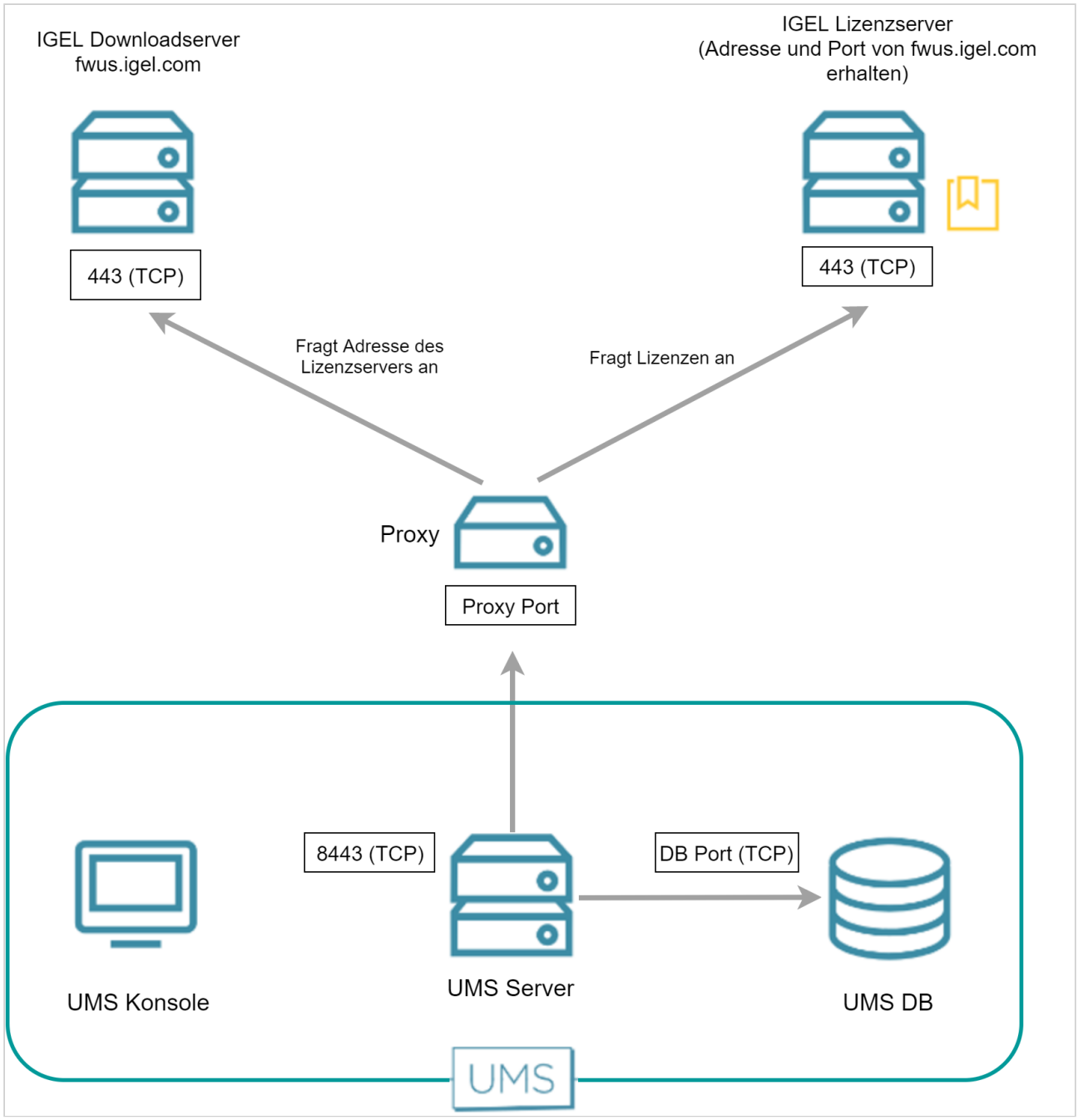
Die folgende Abbildung veranschaulicht die Kommunikation zwischen dem UMS Server und dem IGEL Lizenzserver:



Über Proxyserver

Wenn ein Proxyserver zwischen die UMS und den IGEL Lizenzserver geschaltet ist, muss der Port für den Proxy unter **UMS Administration > Globale Konfiguration > Proxyserver** angegeben werden.

⚠ Wenn mehrere Proxies konfiguriert sind, stellen Sie sicher, dass Sie denjenigen auswählen, der für die Lizenzierung definiert ist.



UMS sendet neue Einstellungen an die Geräte

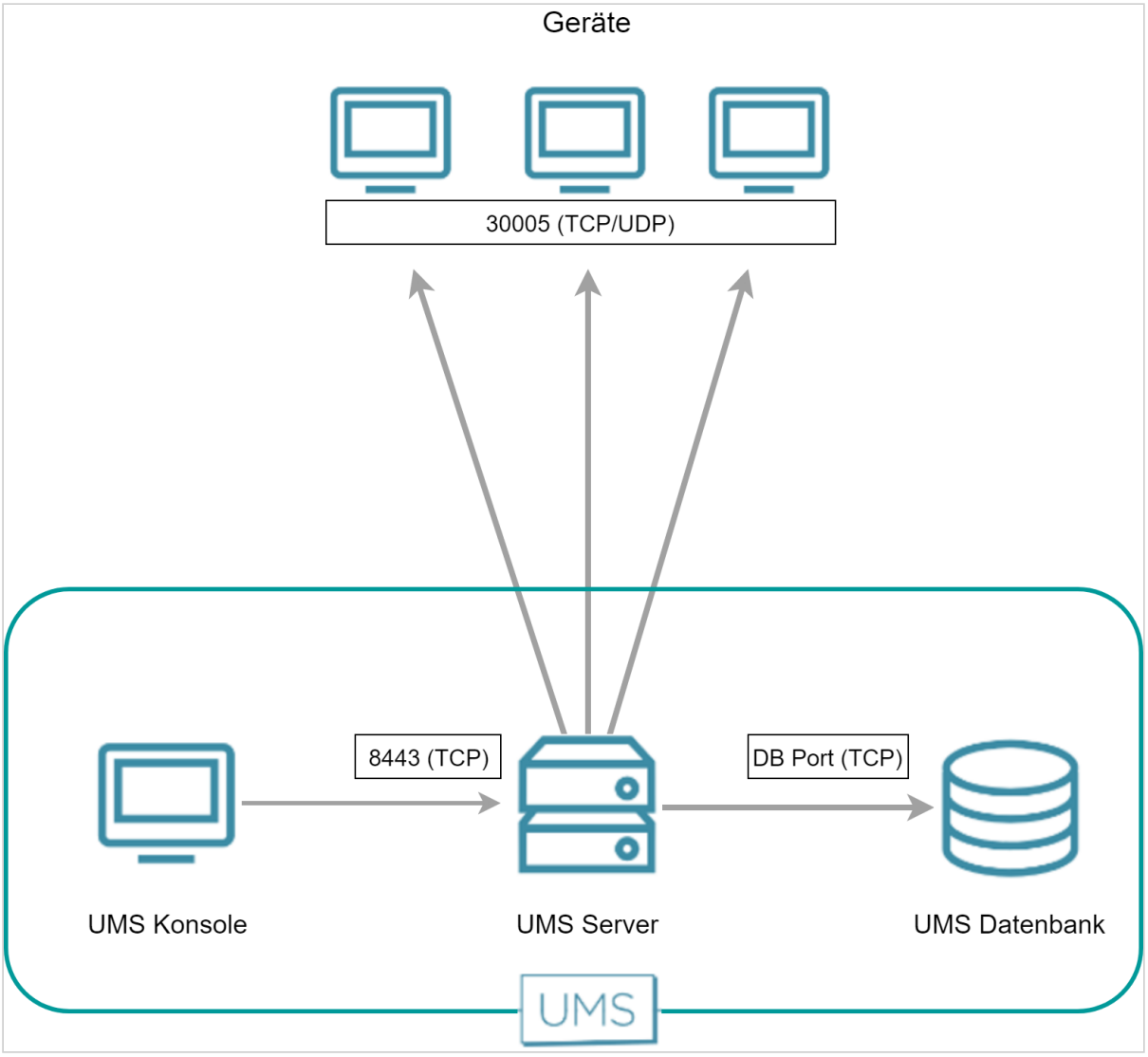
IGEL OS 12

Bei IGEL OS 12-Geräten wird für die Übertragung von Lizenzen kein zusätzlicher Kanal geöffnet. Es wird ein vorhandener WebSocket (TCP 8443) verwendet.

IGEL OS 11 oder früher

Nachdem die Lizenzen vom Lizenzserver bezogen wurden, sendet die UMS neue Einstellungen an jeden betroffenen Geräten, einschließlich eines Downloadlinks für die Lizenzdateien. Das Gerät empfängt auf Port 30005.

Die folgende Abbildung veranschaulicht die Kommunikation zwischen der UMS und dem Gerät:



Geräte kontaktieren die UMS, um Lizenzdateien herunterzuladen

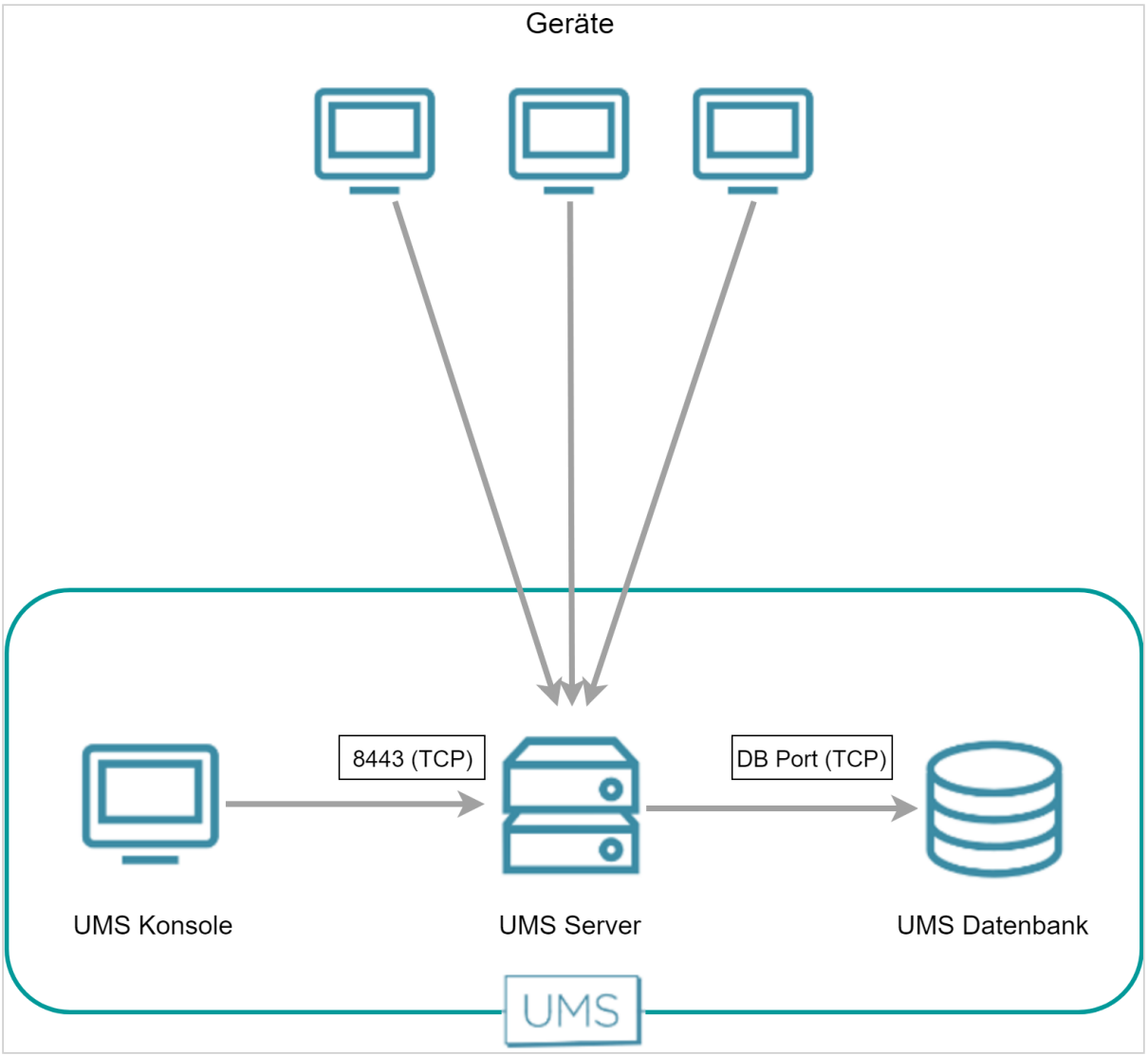
IGEL OS 12

Bei IGEL OS 12-Geräten wird für die Übertragung von Lizenzen kein zusätzlicher Kanal geöffnet. Es wird ein vorhandener WebSocket (TCP 8443) verwendet.

IGEL OS 11 oder früher

Die Geräte wurden von der UMS darüber informiert, dass Lizenzdateien zum Download bereit stehen. Um nun die Lizenzdateien aus der UMS zu holen, senden die Geräte eine HTTPS-Anfrage an den UMS Server. Der UMS Server empfängt auf Port 8443.

Die folgende Abbildung veranschaulicht die Kommunikation zwischen den Geräten und der UMS:

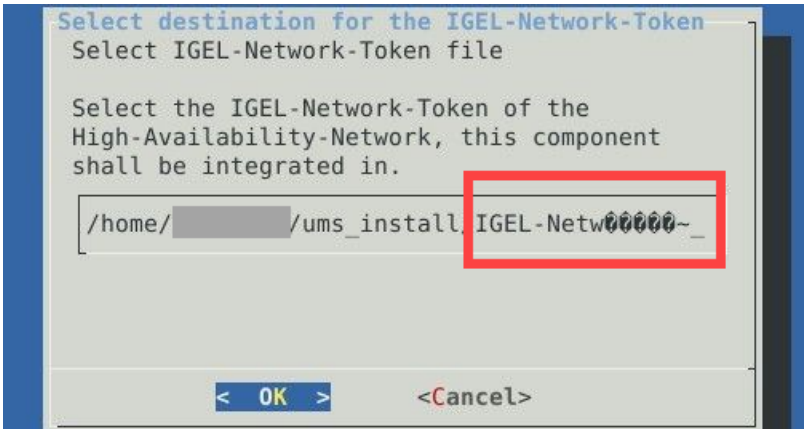


UMS Installation

Sonderzeichen während der UMS Installation unter Linux verwenden

Frage

Warum sehe ich seltsame Symbole im UMS Installer unter Linux, z. B. beim Speichern / Hochladen des IGEL Netzwerktokens?



Antwort

Wenn Sie sprachspezifische Zeichen, z. B. Umlaute (`ä` , `ö` , usw.), für die UMS Installation unter Linux verwenden wollen, müssen folgende Bedingungen erfüllt sein:

- Das korrekte Locale für die Sprache muss eingestellt werden
- Das Systemgebietsschema (system locale) muss ebenfalls korrekt eingestellt sein

▶ Führen Sie den folgenden Befehl aus, um die verfügbaren Gebietsschemata aufzulisten: `locale -a`

▶ Wenn das erforderliche Gebietsschema nicht aufgeführt ist, können Sie es wie folgt generieren und als Standardgebietsschema für Ihr System festlegen (Beispiel für Deutsch):

```
sudo locale-gen de_DE.UTF-8
sudo update-locale LANG=de_DE.UTF-8
```

UMS Installation auf 64-Bit-Systemen

Seit Version 5.09.100 ist IGEL UMS 64-Bit-basiert. Dieser Artikel dient jetzt nur noch zu Informationszwecken.

Frage

Was sind die Voraussetzungen für die Installation der IGEL Universal Management Suite auf 64-Bit-Betriebssystemen?

Antwort

Ab UMS 5.09

Ab UMS Version 5.09 wird die Installation der 32-Bit-Bibliotheken nicht mehr benötigt. Die notwendigen Abhängigkeiten werden automatisch installiert, wenn bei der UMS Installation die entsprechende Option gewählt wurde. Informationen zur UMS Installation finden Sie unter IGEL UMS Installation (see page 246).

Ab UMS 5.07.100

Ab UMS Version 5.07.100 werden die benötigten 32-Bit-Bibliotheken automatisch vom UMS Installer installiert, falls die entsprechende Option während der Installation der UMS gewählt wurde.

Vor UMS 5.07.100

- Windows: Verwenden Sie den 32-Bit-Kompatibilitätsmodus (der standardmäßig aktiviert ist), bevor Sie IGEL UMS installieren (z. B. auf Windows Server 2008 R2).
  Sehen Sie auch MSDN: "Running 32-bit Applications"[2]

- Linux (amd64/x86_64): Installieren Sie die 32-Bit-Kompatibilitätspakete, bevor Sie IGEL UMS installieren.
  Beispiele mit Ubuntu folgen unten, ansonsten siehe:
  UMS auf Red Hat Enterprise Linux (RHEL) 7.3 installieren (see page 261)
  UMS auf Oracle Linux Server installieren (see page 263)

  Beispiel mit Ubuntu 14.04 LTS 64-Bit:

```
# add i386 support
sudo dpkg --add-architecture i386
sudo apt-get update
# install libraries
sudo apt-get install lib32z1 \ lib32ncurses5 \ lib32bz2-1.0 \ libx
```

2 https://msdn.microsoft.com/en-us/library/aa384249%28VS.85%29.aspx

```
tst6:i386 \ libxinerama1:i386 \ libxi6:i386 \ libxext6:i386 \ libx
render1:i386
```

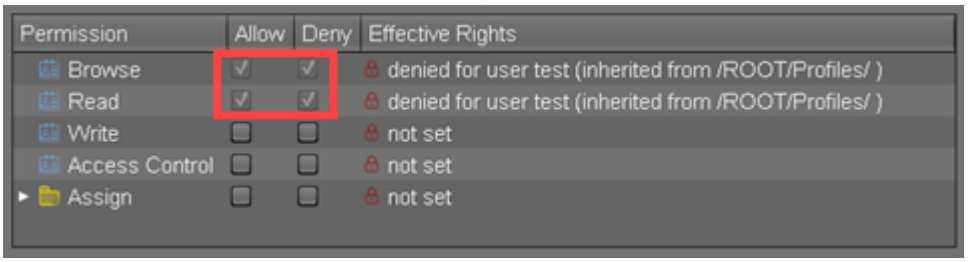
Beispiel mit Ubuntu 16.04 LTS 64-Bit:

```
# add i386 support
sudo dpkg --add-architecture i386
sudo apt-get update
# install libraries
sudo apt-get install lib32z1 \ lib32ncurses5 \ libbz2-1.0:i386 \ l
ibxtst6:i386 \ libxinerama1:i386 \ libxi6:i386 \ libxext6:i386 \ li
bxrender1:i386
```

Keine Berechtigungen nach dem UMS Update

Symptom

Sie haben die UMS auf Version 6.05.100 oder höher aktualisiert und haben keine Berechtigungen mehr für einen Objekt-/Baumknoten in der UMS. Im Dialog **Berechtigungen** sind die beiden Kontrollkästchen **Zulassen** und **Verweigern** aktiviert, aber nicht editierbar:

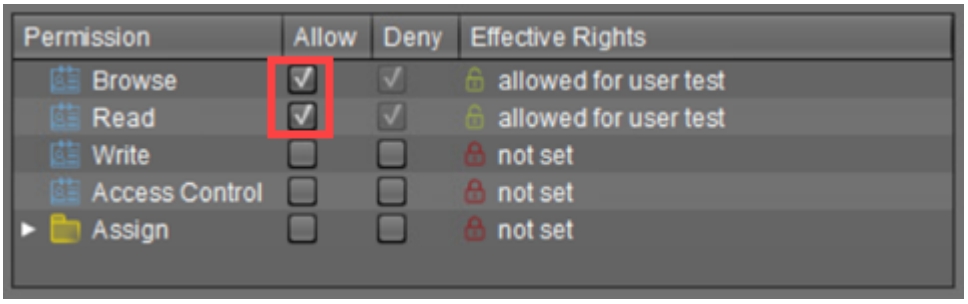


Umgebung

- UMS 6.05.100 oder höher

Problem

Vor UMS 6.05.100 konnten Berechtigungen für einen Unterknoten gewährt werden, selbst wenn sie für einen Oberknoten verweigert wurden.



Mit der UMS Version 6.05.100 hat sich die Evaluierung von UMS Berechtigungen geändert: Wenn Sie auf einen Knoten **Verweigern** setzen, können Sie einen Unterknoten nicht mehr auf **Zulassen** setzen. Das Kontrollkästchen **Zulassen** ist in dem Fall nicht editierbar.

Lösung

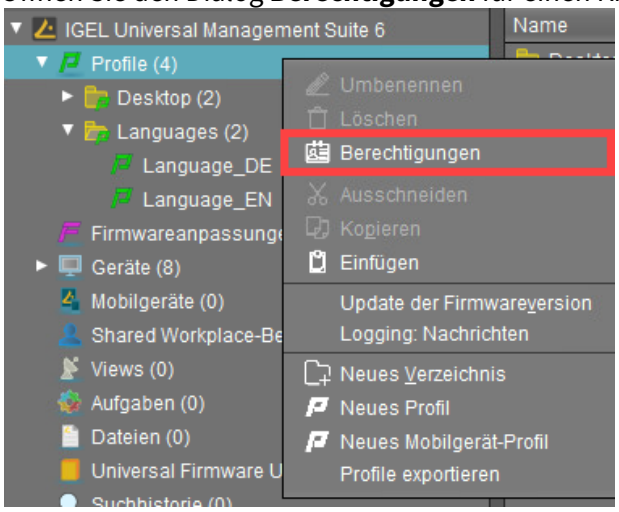
▶ Überprüfen Sie die Berechtigungen im Dialog **Berechtigungen**. Wenn die Berechtigungen **Zulassen** für einen Unterknoten erteilt werden sollen, setzen Sie keine Berechtigungen für den Oberknoten.

Wenn die Berechtigungen nicht gesetzt sind, ist das Verhalten wie bei **Verweigern**. Daher hat der Benutzer keine Zugriffsrechte auf den Knoten, kann aber bis zum Unterknoten navigieren.

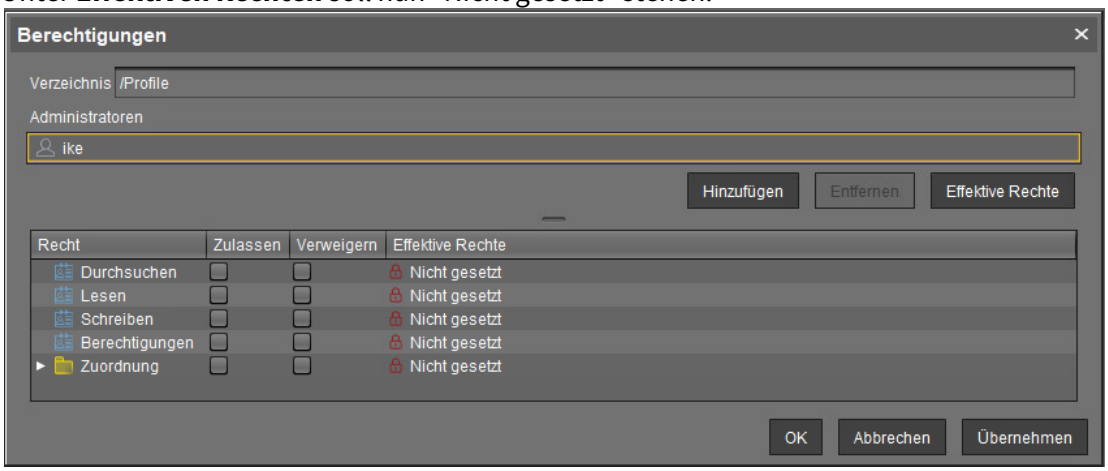
Beispiel:

Der Benutzer sollte nur Zugriffsrechte auf den Profilordner "Languages" und dessen Inhalt haben:

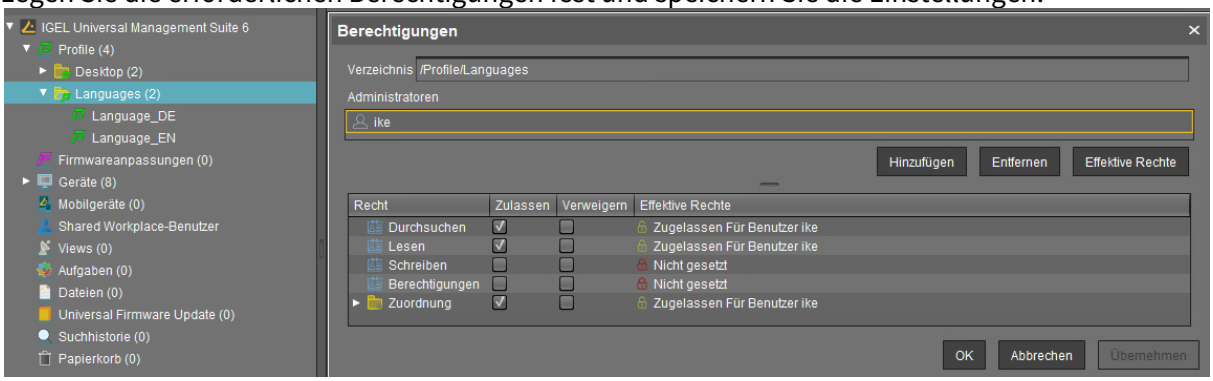
1. Öffnen Sie den Dialog **Berechtigungen** für einen Knoten, in diesem Fall **Profile**.



2. Deaktivieren Sie die Kontrollkästchen **Zulassen** und **Verweigern**.
   Unter **Effektiven Rechten** soll nun "Nicht gesetzt" stehen.



3. Öffnen Sie den Dialog **Berechtigungen** für einen Unterknoten, für den Zugriffsrechte erteilt werden sollen. In unserem Fall ist dies der Ordner "Languages".
4. Legen Sie die erforderlichen Berechtigungen fest und speichern Sie die Einstellungen.



Der Benutzer kann nur bis zu dem Unterknoten "Languages" navigieren, für den die Zugriffsrechte erteilt wurden.

Ungültiges Webzertifikat und Fehler bei der Geräteregistrierung nach der Installation der IGEL UMS 12 unter Linux

Sie haben unter Linux die IGEL Universal Management Suite (UMS) 12 installiert oder Ihre bestehende UMS-Installation auf UMS 12 aktualisiert und haben nun verschiedene Probleme, z.B. mit dem Scannen und Registrieren von IGEL OS 12-Geräten.

Symptom

Nach der Installation von UMS 12 unter Linux haben Sie Probleme mit der automatischen oder manuellen Geräteregistrierung, der Anmeldung bei der UMS Web App, usw.

Auf der Geräteseite sehen Sie den folgenden Fehler (z. B. beim Ausführen des Befehls `journalctl -f` beim Versuch, das Gerät zu registrieren):

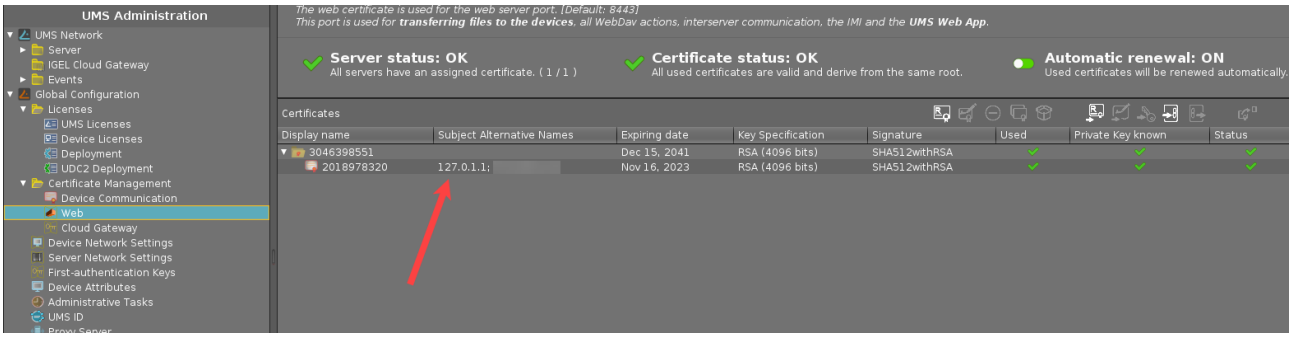
```
ERROR: Failed to verify certificate... IP address mismatch
```

Umgebung

- IGEL UMS 12 unter Linux

Problem

Bei Neu- oder Update-Installationen auf einem Linux-Host kann die von JRE ermittelte IP-Adresse oft falsch sein (z.B. Standard-IP: 127.0.1.1). Wurde bei der Installation / dem Update im UMS-Installer nicht die korrekte IP des UMS Servers angegeben, so führt dies zu ungültigen UMS Zertifikaten.



Lösung

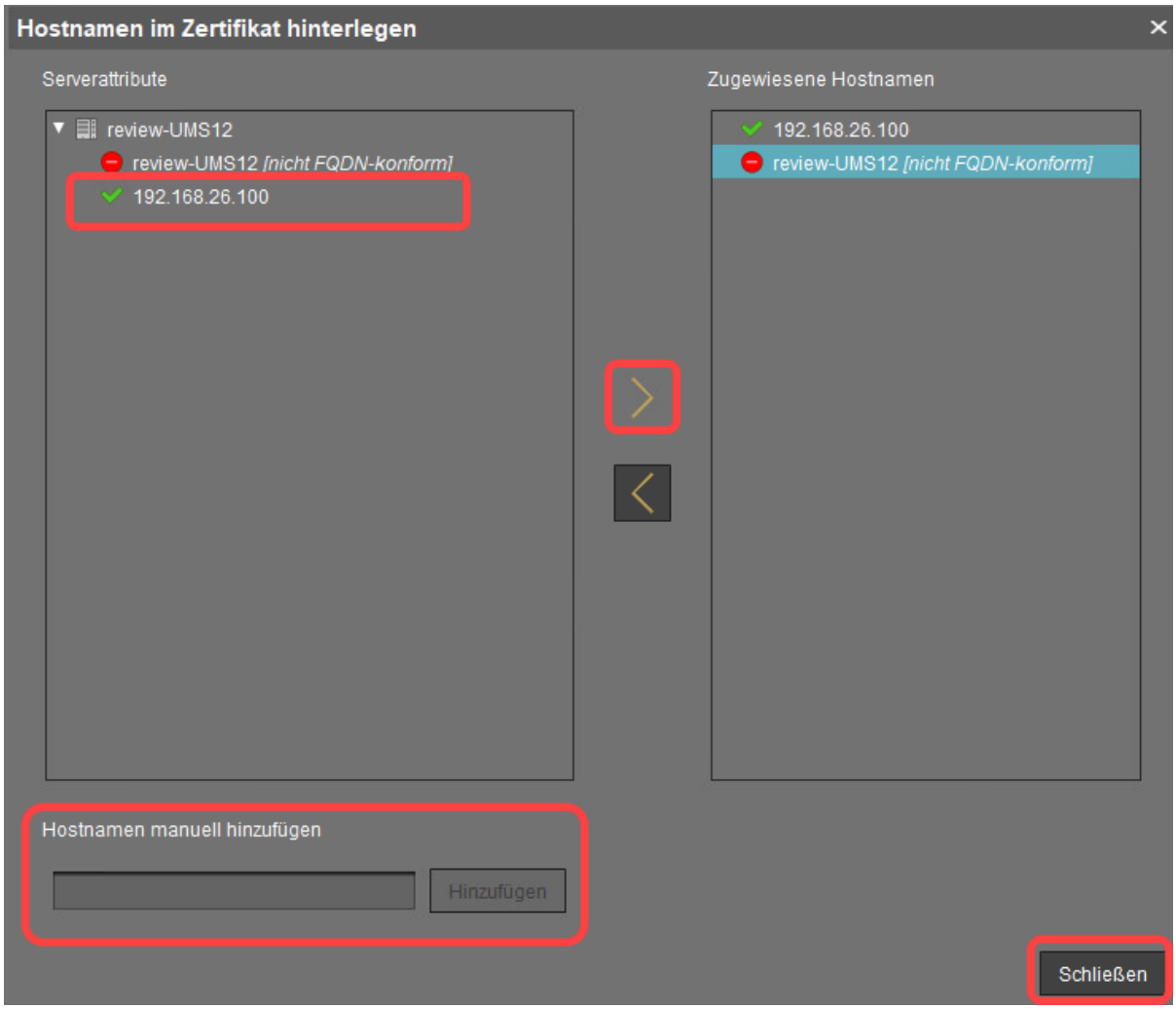
Sie müssen ein neues Zertifikat generieren:

1. Gehen Sie in der UMS Konsole zu **UMS Administration > Globale Konfiguration > Zertifikatsverwaltung > Web**.

2. Wählen Sie das vorhandene Zertifikat aus und klicken Sie **Zertifikat erneuern**  .

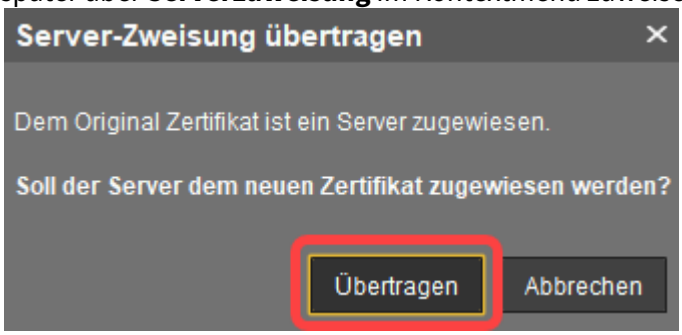
3. Füllen Sie im Dialog **Signiertes Zertifikat generieren** die leeren Felder aus (falls vorhanden); alle anderen Einstellungen können Sie unverändert lassen. Klicken Sie **Hostnamen verwalten**.

4. Prüfen Sie im Dialog **Hostnamen im Zertifikat hinterlegen**, ob "localhost" und alle IP-Adressen und FQDNs (Fully Qualified Domain Names), unter denen Ihr Server erreichbar ist, unter **Zugewiesene Hostnamen** angezeigt werden. Falls nicht, fügen Sie die fehlenden IP-Adressen und FQDNs unter **Hostnamen manuell hinzufügen** hinzu.
   Hinweis: Unter **Zugewiesene Hostnamen** dürfen nur FQDN-konforme Namen vorhanden sein. Entfernen Sie alle nicht FQDN-konformen Namen, falls es welche gibt, mit einer Pfeilschaltfläche.



5. Klicken Sie **Ok**.

6. Klicken Sie im Dialog **Server-Zuweisung übertragen** auf **Übertragen**.
   Hinweis: Wenn Sie sich nicht sicher sind, können Sie **Abbrechen** klicken und das erstellte Zertifikat später über **Serverzuweisung** im Kontextmenü zuweisen.



Das neue Zertifikat wird erstellt und für den Server verwendet.

Es wird auch empfohlen, die Linux OS Datei `/etc/hosts` zu überprüfen. Wenn dort falsche Einträge wie 127.0.1.1 vorhanden sind, ändern Sie diese in die korrekte IP Ihres UMS Servers und den richtigen Servernamen.

Anpassung

Regeln für die Benutzerautorisierung

Problem

In der IGEL UMS möchten Sie Administratoren Berechtigungen oder Rollen entsprechend den verschiedenen Verantwortlichkeiten zuweisen.

Grund

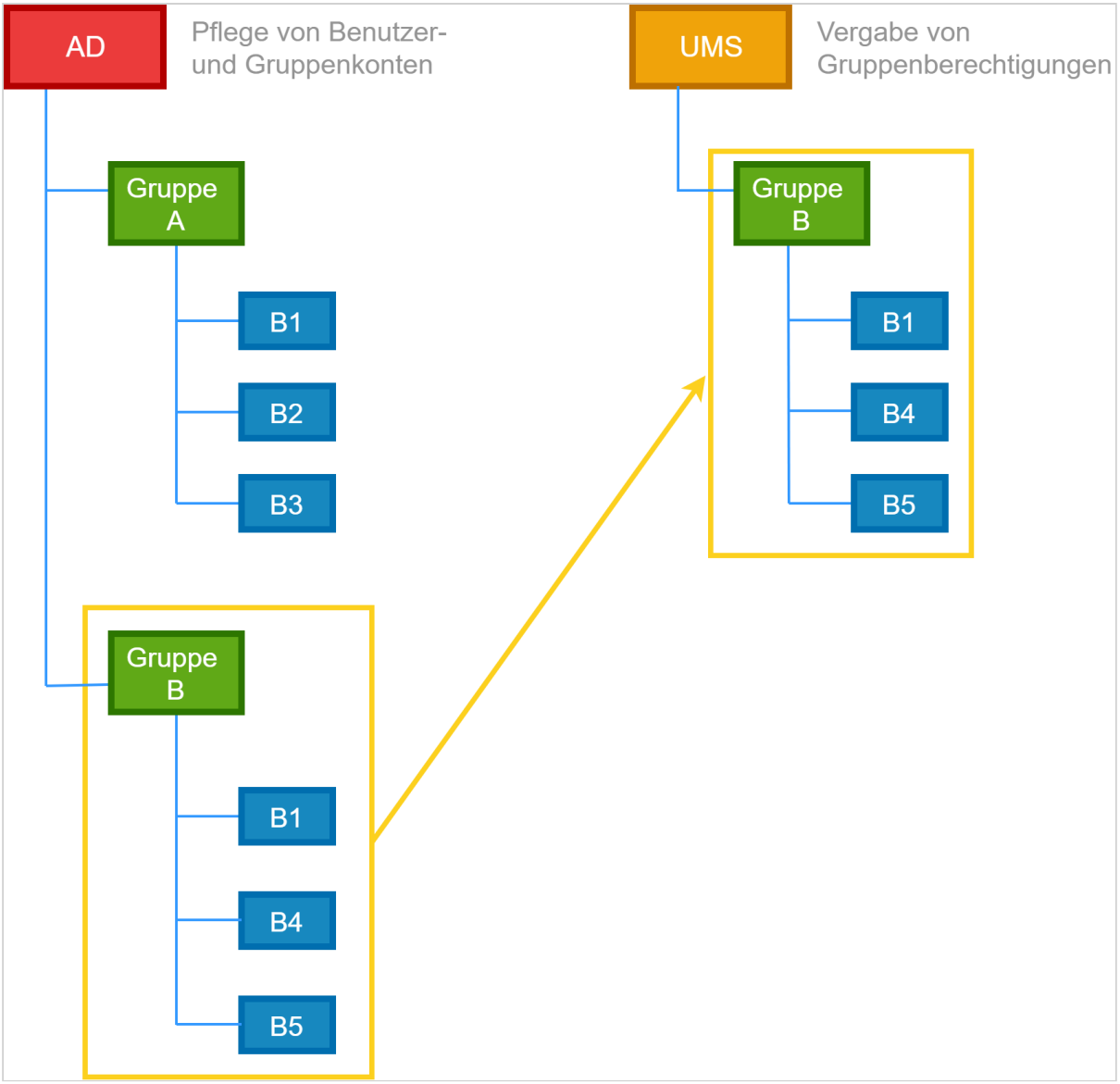
In der IGEL UMS können Sie Benutzer- oder Administratorkonten erstellen und ihnen Regeln zuweisen, aber es ist nicht möglich, Rollen zuzuordnen.

Sie möchten Administratoren nach ihren Aufgaben gruppieren, um eine klar strukturierte Verwaltung der Benutzerrechte zu erreichen.

In Ihrem Unternehmen führen Sie bereits Mitarbeiterkonten über ein Active Directory oder LDAP.

Lösung

Wir empfehlen, die UMS mit den Benutzerkonten des Active Directory zu verbinden. Sie pflegen die Benutzer- und Gruppenkonten nur im Active Directory. Im UMS weisen Sie den importierten Gruppen Rechte zu.



Übertragen von Active Directory-Gruppen an die UMS und Zuweisen von Berechtigungen und Rollen:

▶ Klicken Sie **UMS Administration > Globale Konfiguration > Active Directory /LDAP** um Ihr Active Directory zu integrieren.

> ⓘ Sie können Administrative Benutzer / UMS-Administratoren sowohl aus einem Active Directory als auch aus einem LDAP importieren.

▶ Klicken Sie in der UMS Konsole **System > Administratorkonten > Importieren**, um Gruppen aus der Struktur Ihres Active Directory zu importieren.

Der erfolgreiche Import einer Gruppe kann nicht rückgängig gemacht werden. Sie müssen eine falsch angelegte UMS-Gruppe in der Verwaltung "Administratorkonto" manuell löschen. Der Name der importierten Active Directory-Gruppe wird aus dem Konto übernommen.

▶ Zuordnung von Rollen zu Gruppen in der IGEL UMS auf Basis von Berechtigungsregeln:

- Klicken Sie **System > Administratorkonten > Gruppen > Bearbeiten** um allgemeine Gruppenrechte direkt zuzuweisen.
- Vergeben Sie objektbezogene Zugriffsrechte über **Objektberechtigungen** und wählen Sie Zugriffskontrolle im Kontextmenü eines beliebigen Objekts.

Auf diese Weise können Sie den Administratoren der UMS bestimmte Rollen entsprechend ihrer Gruppenzugehörigkeit zuweisen.

Bitte beachten Sie:

- Berechtigungen werden von einem übergeordneten Verzeichnis an ein Unterverzeichnis oder an ein untergeordnetes Objekt vererbt.
- Es ist möglich, indirekte Rechte zu ändern, d. h. Rechte, die durch Gruppenzuordnung vergeben werden. Direkt zugewiesene Rechte haben jedoch Vorrang vor indirekt zugewiesenen Rechten.
- Ein Administrator kann Mitglied verschiedener Gruppen sein und erhält die entsprechenden Rechte. Sind sie widersprüchlich, hat der Entzug eines Rechts Vorrang vor der Erlaubnis. Wenn ein Verbot für eine Klage oder einen Gegenstand einer Gruppe erlassen wird, überschreibt es eine beliebige Anzahl von Rechten anderer Gruppen.
- Klicken Sie auf **Effektive Rechte**, um weitere Details zur Regelbestimmung zu erhalten, z. B. wenn eine Berechtigung direkt erteilt wurde oder wenn sie von einer Gruppe oder durch eine Vererbung innerhalb einer Baumstruktur zugewiesen wurde.

Benutzerrechte über die UMS verwalten

Verwendungszweck

Es ist notwendig, die Berechtigungen der Geräte-Benutzer global zu verwalten, z. B. für die Bearbeitung von Systeminformationen.

Lösung

Verwenden Sie die Funktion **Berechtigungen** in der UMS.

Zusätzliche Information

Es gibt verschiedene Orte, um den Dialog **Berechtigungen** zu öffnen:

- Im Hauptmenü unter **Bearbeiten > Berechtigungen**
- In der Symbolleiste unter 
- Im Kontextmenü eines Gerätes oder eines Geräteordners unter **Berechtigungen**

Endbenutzerberechtigungen definieren

1. Klicken Sie im Kontextmenü eines Gerätes (Ordner) auf **Berechtigungen**.
   Der Dialog **Berechtigungen** öffnet sich.
2. Klicken Sie auf **Hinzufügen**, um einen neuen Benutzer/Gruppe auszuwählen.
3. Die entsprechenden **effektiven Rechte** werden im unteren Teil der Maske aufgelistet.
4. Erlauben **(zulassen)** oder **verweigern** Sie die Berechtigungen der ausgewählten Gruppe oder des ausgewählten Benutzers für die ausgewählten Geräte.
5. Bestätigen Sie die Einstellungen mit **Ok.**
6. Klicken Sie **Aktualisieren** in der Konsole, um die Änderungen in der UMS zu übernehmen.

   > Wenn Sie die Rechte der registrierten Benutzer geändert haben, werden diese erst nach einer Aktualisierung wirksam.

   Weitere Details zu den Autorisierungsregeln finden Sie in unserem How-To: Regeln für die Benutzerautorisierung (see page 79).

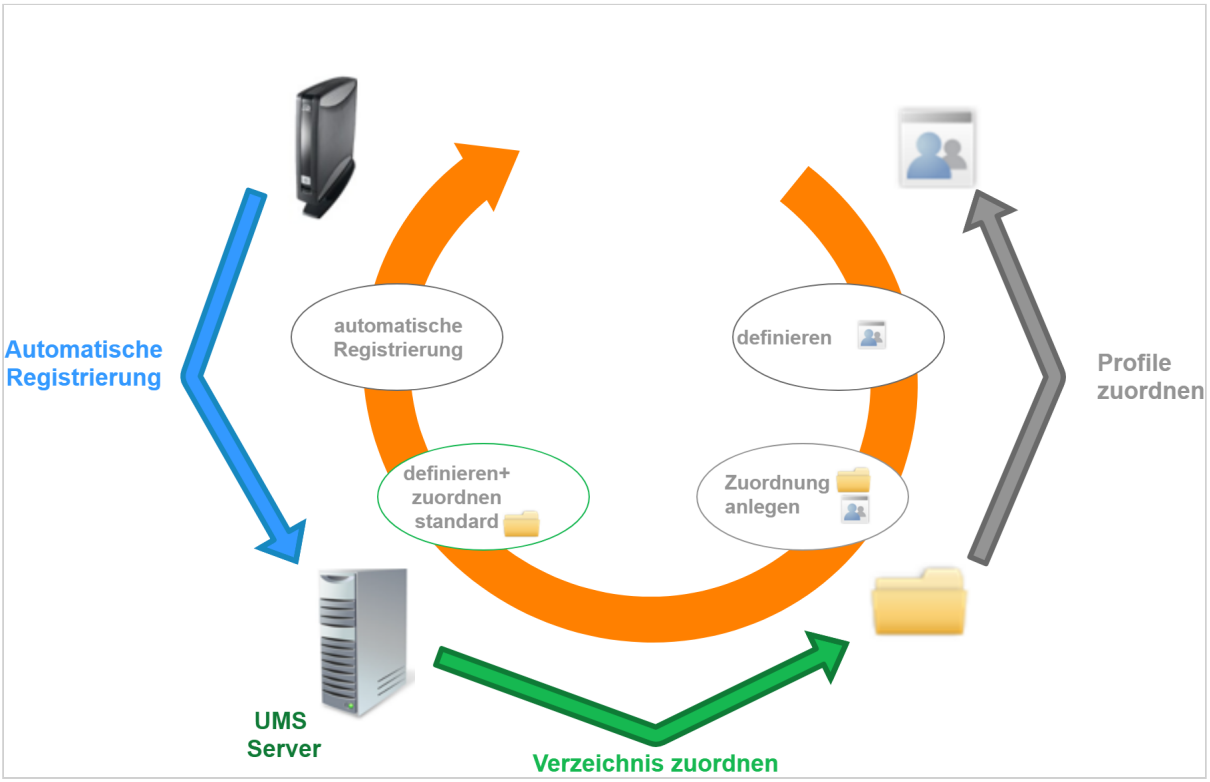
> Zugriffsrechte auf Objekte oder Aktionen innerhalb der IGEL UMS sind den Administratorkonten und -gruppen zugeordnet. Die Rechte des Datenbank-Benutzerkontos können nicht eingeschränkt werden. Sie werden bei der Installation oder beim Einrichten der Datenquelle erstellt. Das Konto hat immer volle Zugriffsrechte in der UMS.

Roll-out-Prozess in der IGEL UMS automatisieren

Sie möchten die IGEL Universal Management Suite (UMS) so einrichten, dass neue Geräte direkt im richtigen Verzeichnis abgelegt werden und automatisch die richtigen Konfigurationen zugeordnet werden. Mit Zero Touch Deployment werden Geräte beim Rollout automatisch entsprechend den Profilen konfiguriert, ohne größeren Verwaltungsaufwand.

Die Idee von Zero Touch Deployment bedeutet automatische Geräteregistrierung mit automatischer Zuweisung von Profilen nach voreingestellten Verzeichnisregeln.

Am Ende wird das Gerät automatisch in der UMS registriert, automatisch dem richtigen Verzeichnis zugeordnet und automatisch mit den gültigen Profilen verknüpft. Um diesen automatisierten Prozess vorzubereiten, müssen Sie den umgekehrten Weg gehen. Definieren Sie zunächst die Profile, ordnen Sie sie den Verzeichnissen zu, erstellen Sie dann Vorgabeverzeichnisregeln und automatisieren Sie die Registrierung.



Vorbereitung des automatischen Rollouts

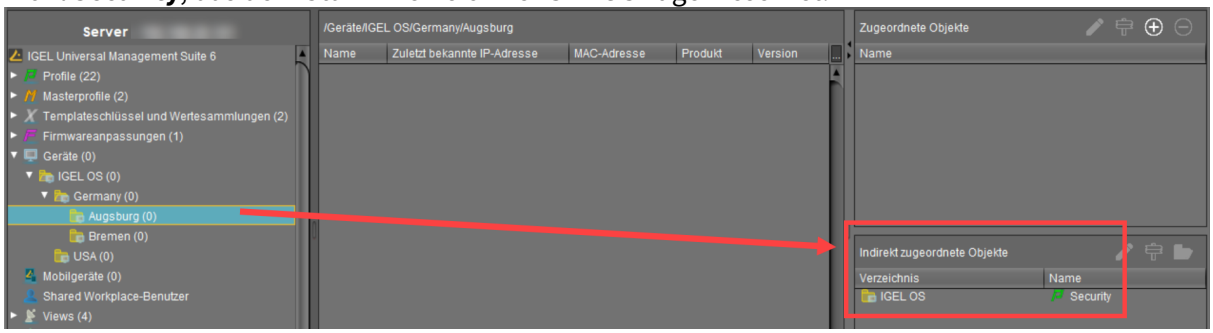
Konfigurieren Sie Ihre Geräte global und weisen Sie Profile indirekt über ein übergeordnetes Verzeichnis zu:

1. Erstellen Sie ein neues Stammverzeichnis, z. B. **IGEL OS**.
   Wie Sie ein Geräteverzeichnis erstellen können, erfahren Sie unter Verzeichnis in der IGEL UMS erstellen (see page 456).

2. Ordnen Sie diesem Stammverzeichnis bestimmte Profile zu, z. B. **Security**.
   Informationen zum Zuweisen von Profilen finden Sie unter Wie kann ich IGEL UMS Profile zuweisen? (see page 379) Siehe auch Priorisierung von Profilen in der IGEL UMS (see page 398).
   Ausführliche Informationen zu Profilen finden Sie unter Profile in der IGEL UMS (see page 365).

3. Verschieben Sie Ihre Geräte oder Ihre Verzeichnisse mit Geräten in dieses Stammverzeichnis.
   Diese Geräte erben die dem Stammverzeichnis zugeordneten Profile.

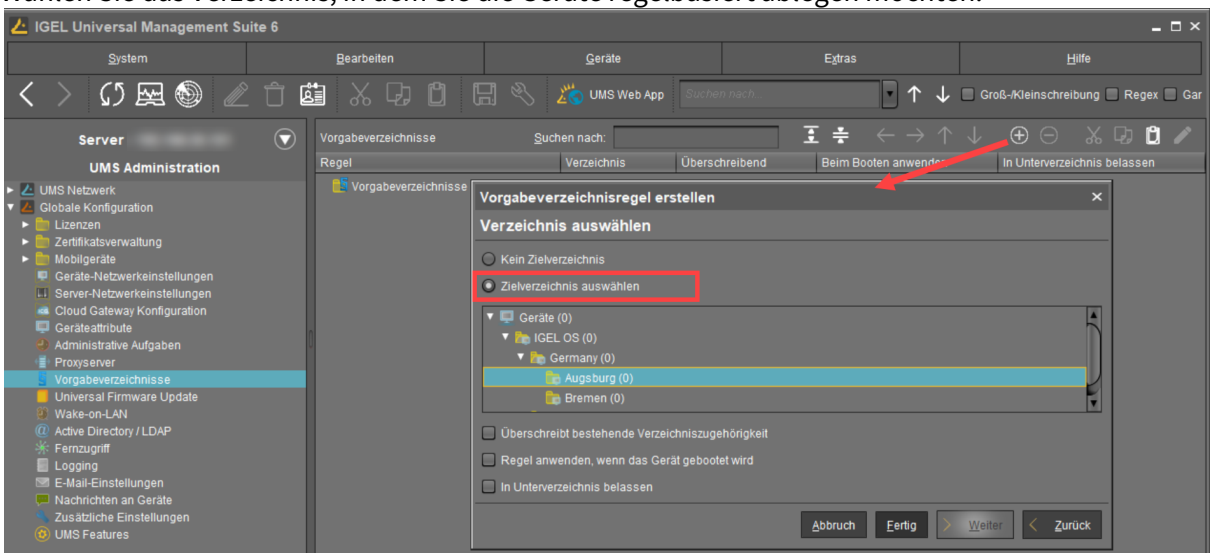
   Beispiel: Geräte, die bei der Registrierung in das Verzeichnis **Augsburg** abgelegt werden, erben das Profil **Security**, das dem Stammverzeichnis **IGEL OS** zugewiesen ist:

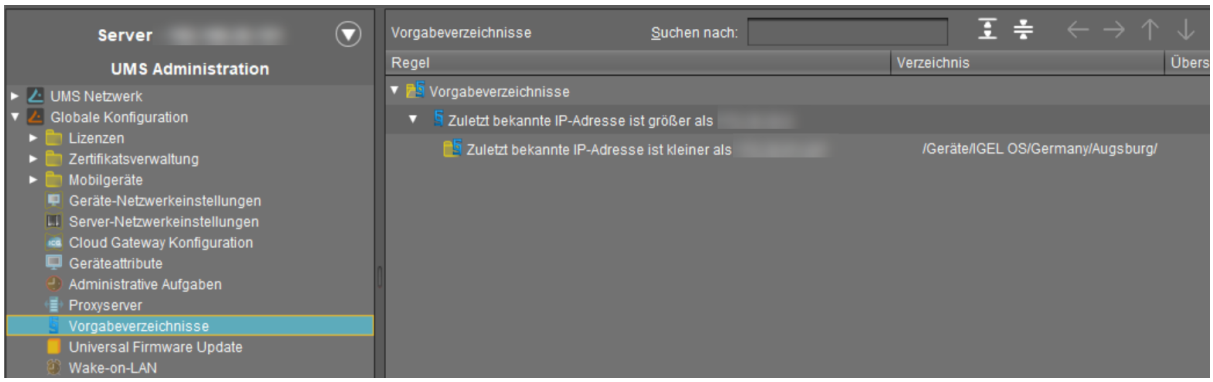


Automatisierung des Rollouts

1. Klicken Sie auf **UMS Administration > Globale Konfiguration > Vorgabeverzeichnisse**, um eine neue Vorgabeverzeichnisregel zu erstellen.
   Ausführliche Informationen zu Vorgabeverzeichnisregeln finden Sie unter Vorgabeverzeichnisse (see page 643).

2. Wählen Sie das Verzeichnis, in dem Sie die Geräte regelbasiert ablegen möchten.



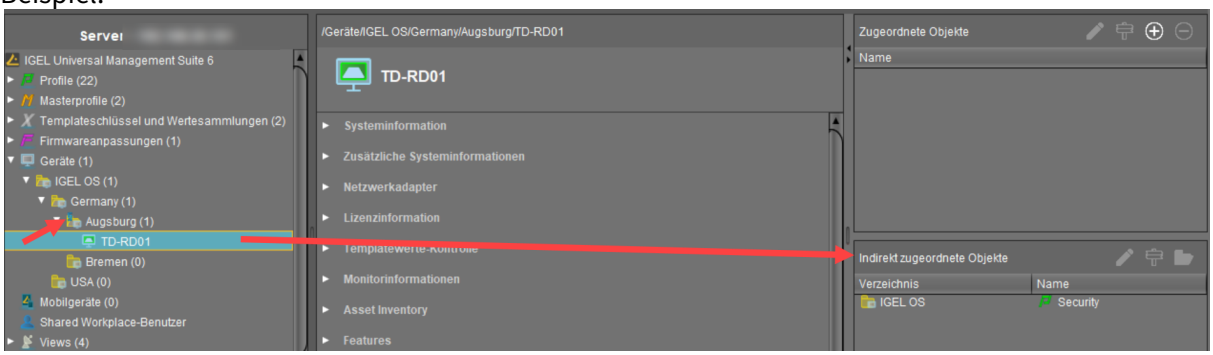


3. Konfigurieren Sie Ihren DNS- oder DHCP-Server und aktivieren Sie automatische Registrierung von Geräten wie unter Geräte automatisch an der IGEL UMS registrieren (see page 337) beschrieben.

   > ⓘ Wir empfehlen, die automatische Registrierung nach dem Rollout zu deaktivieren, damit keine unbekannten Geräte ohne Ihre Kontrolle registriert werden und sensitive Daten erhalten können.

4. Starten Sie Ihre Geräte. Sie werden automatisch am UMS Server registriert.
   Dank der Vorgabeverzeichnisregel werden diese Geräte im richtigen Verzeichnis abgelegt und erhalten automatisch die richtigen Profile.

   Beispiel:



Ähnliche Themen

Wenn Sie Strukturtags für die Automatisierung des Rollouts verwenden möchten: Verwendung von Struktur-Tags mit IGEL OS 11 Geräten (see page 86)

Wenn Sie Probleme mit der Geräteregistrierung haben: Troubleshooting: Die Registrierung eines Geräts über Suche nach Geräten schlägt fehl (see page 165)

Verwendung von Struktur-Tags mit IGEL OS 11 Geräten

Problem

Beim automatischen Rollout von Geräten kann es schwierig sein, jedes einzelne dem gewünschten Ordner in der Universal Management Suite (UMS) zuzuordnen.

Ziel

Neu registrierte Geräte erhalten automatisch die Informationen, wo sie im Strukturbaum der UMS platziert werden sollen.

Die UMS verfügt über verschiedene Regeln, um ein neu registriertes Gerät in einen Ordner des Strukturbaums zu legen.

Lösung

Eine Lösung ist die Verwendung eines Struktur-Tags, einer an das Gerät gebundenen Zeichenkette, die an die UMS übertragen wird. Sie kann den Geräten entweder über eine DHCP-Option oder im lokalen Setup zugewiesen werden.

1. Verwenden Sie ein Struktur-Tag in Ihren Standardverzeichnisregeln unter **UMS Administration > Globale Konfiguration > Vorgabeverzeichnisse**.
   Erfahren Sie mehr im UMS-Handbuch: Vorgabeverzeichnisse.
2. Weisen Sie das Struktur-Tag einem Gert zu, entweder manuell oder über DHCP:
   Struktur-Tag auf dem Gerät manuell zuweisen
   a. Gehen Sie im **Setup** unter **System > Fernadministration.**
   b. Geben Sie den Wert des Struktur-Tags unter **Strukturtag** ein.
   c. Klicken Sie **Ok.**

   Struktur-Tag per DHCP Server zuweisen

   Verwenden Sie je nach der IGEL OS Version Ihrer Endgeräte die entsprechende DHCP-Option:

   - IGEL OS 11.03.500 oder niedriger: Verwenden Sie DHCP-Option 226, um den Wert des Tags auf die Geräte zu verteilen. Legen Sie die DHCP-Option 224 als Zeichenfolge fest, nicht als DWORD.
   - IGEL OS 11.04.100 oder höher: Alternativ können Sie die DHCP-Option 43 (encapsulated vendor-specific options) verwenden, um die DHCP-Option 226 (Name: "umsstructuretag") an die richtigen Endgeräte zu senden. Ein Endgerät mit IGEL OS 11.04.100 oder höher sendet die Option 60 (vendor class identifier) mit `igel-dhcp-1` als Wert.

     > Eine IGEL-spezifische DHCP-Option, die in DHCP-Option 43 gesendet wird, überschreibt eine entsprechende DHCP-Option, die im globalen Namensraum gesendet wird. Die DHCP-Optionen 1, 224 und 226 können in Option 43 eingebettet werden.

Sie können verhindern, dass eine DHCP-Option 226, die im globalen Namensraum gesendet wurde, interpretiert wird. Um dies zu erreichen, müssen Sie Option 1 (Name "exklusiv", Typ Byte, Wert 1) zur DHCP-Option 43 hinzufügen.

IGEL Custom Partitions über die UMS bereitstellen

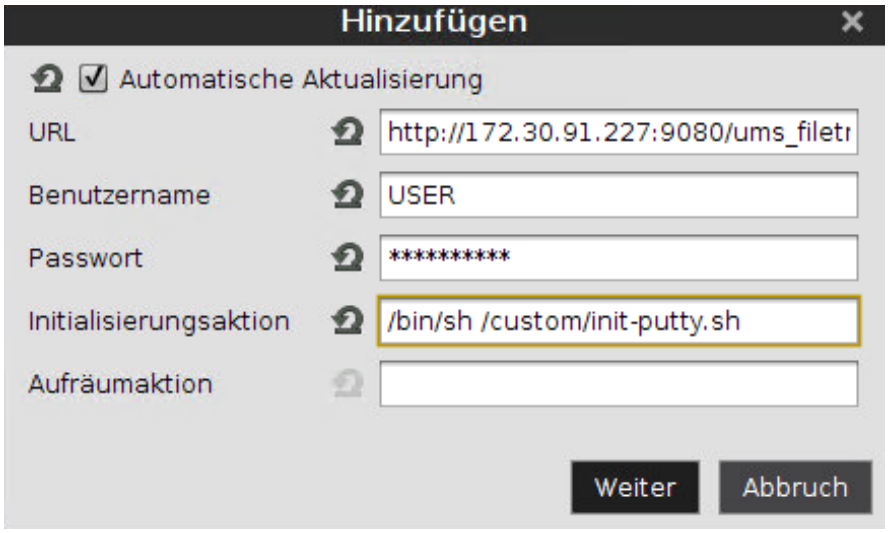
Ziel

Sie möchten eine benutzerdefinierte Partition, die Sie von IGEL erhalten haben, über die Universal Management Suite (UMS) auf einer Reihe von Geräten bereitstellen.

Lösung

> Die hier beschriebene Vorgehensweise ist nur für die Installation von Custom Partition-Paketen vorgesehen, die von IGEL erstellt wurden.

1. Speichern Sie das `*.zip` -Archiv, das Sie lokal erhalten haben, und entpacken Sie es.
2. Kopieren Sie den Inhalt des Verzeichnisses `target` in das Verzeichnis `ums_filetransfer` a uf dem UMS Server, z. B. `C:\Program Files(x86)\IGEL\RemoteManager\rmguiserver\webapps\ums_filetransfer`
3. Überprüfen Sie die Zugänglichkeit der Daten, indem Sie deren Adresse in einem Webbrowser öffnen, z. B. `http://[ums_server]:9080/ums_filetransfer/[name]/[name].inf`
   Dieser Zugang ist passwortgeschützt, und Sie müssen Ihre UMS-Anmeldeinformationen eingeben.
4. Importieren Sie die Datei `profiles.zip` (im Verzeichnis `igel\profiles` des Pakets) in die UMS über **System > Importieren > Profile importieren.**
   Das importierte Profil sollte nun in der UMS-Konsole unter **Profile** erscheinen.
5. Bearbeiten Sie das Profil und passen Sie die Einstellungen unter **System > Firmwareanpassung > Eigene Partition > Download** an, um die **URL**, den **Benutzernamen** und das **Passwort** für Ihre UMS anzupassen.



6. Ordnen Sie das Profil einem oder mehreren Geräten zu.
7. Starten Sie diese Geräte neu.

UMS Umgebung

Migration eines UMS Servers

Wenn Sie Ihre IGEL Universal Management Suite (UMS) auf einen neuen Server migrieren möchten, finden Sie hier die Anleitungen, Empfehlungen und Tipps zum Migrationsprozess.

Anleitungen für Anwendungsszenarien

Finden Sie ausführliche Anleitungen für die folgenden Migrationsszenarien:

- UMS Server migrieren und die gleiche integrierte Datenquelle beibehalten: Migration eines UMS Server mit derselben Embedded-Datenbank (see page 92)
- UMS mit externer Datenquelle migrieren und die gleiche externe Datenquelle beibehalten: Migration eines UMS Server mit der selben externen Datenbank (see page 96)
- UMS migrieren und die Datenquelle ändern: Mit einer anderen Datenbank (see page 100)

Empfehlungen

- Trennen Sie das Migrations- und das Updatevorgänge.
  Wenn Sie von UMS 12.01 auf 12.03 umsteigen wollen, aktualisieren Sie zuerst die UMS und migrieren Sie danach den Server oder umgekehrt.
- Verwenden Sie die gleiche UMS-ID.
  Die Verbindung zu ILP, App Portal und anderen Diensten ist von der UMS-ID abhängig und würde bei einer Änderung beeinträchtigt werden.
- Verwenden Sie die gleiche Zertifikatskette.
  Wenn sie geändert werden muss, verwenden Sie die alte Kette für die Migration und ändern Sie sie, nachdem die Migration erfolgreich war, oder ändern Sie sie, bevor Sie migrieren.

Tipp

Der Umzug bietet die Möglichkeit, nicht mehr verwendete Daten aus der UMS Datenbank zu entfernen. Sie können z. B.

- Endgeräte löschen, die nicht mehr existieren
- Profile löschen, die nicht mehr verwendet werden
- Dateien und Firmwareupdates entfernen, die nicht mehr benötigt werden

Es wird empfohlen, ein Backup vor der Durchführung der Bereinigung zu erstellen (als Sicherung des laufenden Systems) und ein weiteres nach der Bereinigung.

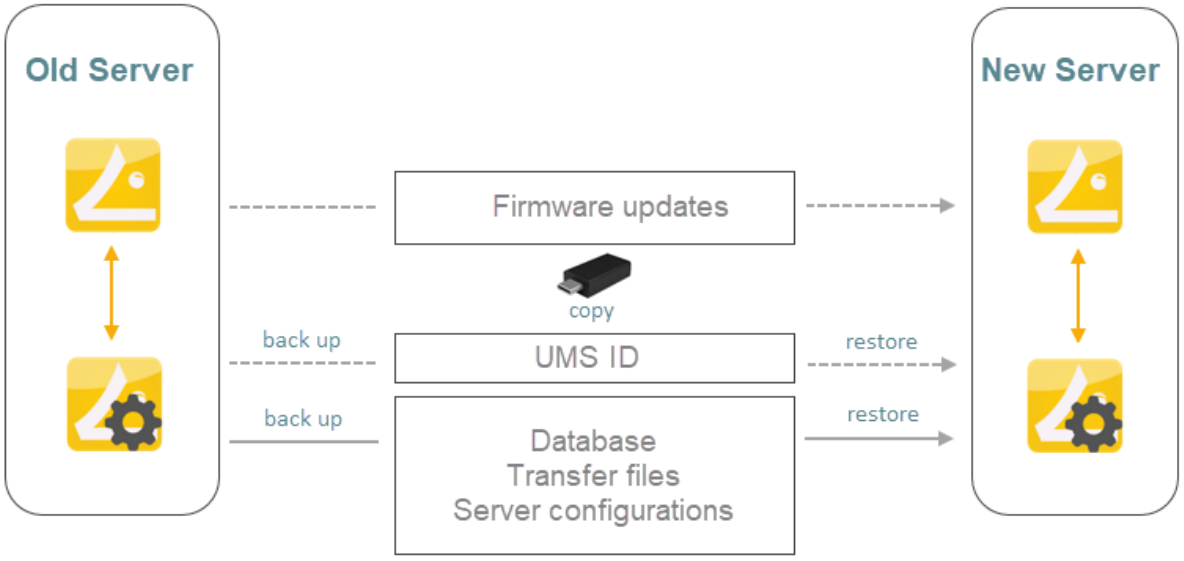
Während der Migration gibt es keine negativen Auswirkungen auf Ihre Endgeräte – sie werden weiter autark arbeiten. Ausnahme: Anmeldung über Shared Workplace (SWP) (see page 951). Details finden Sie unter Welche Features von IGEL OS sind betroffen, wenn die UMS ausfällt?.

Migration eines UMS Server mit derselben Embedded-Datenbank

Anwendungsfall

Sie haben eine UMS Installation mit einer eingebetteten Datenbank und möchten auf einen neuen UMS Server mit der gleichen eingebetteten Datenbank migrieren.

Allgemeiner Überblick



Das Migrationsverfahren umfasst im Allgemeinen die folgenden Schritte:

1. Profil mit der IP des neuen Servers für die Fernadministration erstellen (nur notwendig, wenn Geräte die UMS über IP finden)
2. `IGEL RMGUIServer`-Dienst auf dem alten Server stoppen
3. Ein Backup des alten Servers erstellen. Checkliste für die Backups:
   - ✅ **Datenbank**
   - ✅ **Dateien**
   - ✅ **Serverkonfigurationen** (hostspezifische Serverkonfigurationen, die von den Standardeinstellungen abweichen, sind separat notiert)
   - ✅ **Firmwareupdates**
   - ✅ **UMS-ID**
4. Die erstellten Backups auf den neuen Server übertragen
5. DHCP-Tag und DNS-Alias auf dem neuen Server anpassen (nur erforderlich, wenn Geräte die UMS über DNS/DHCP finden)

Anweisungen

Auf dem alten Server

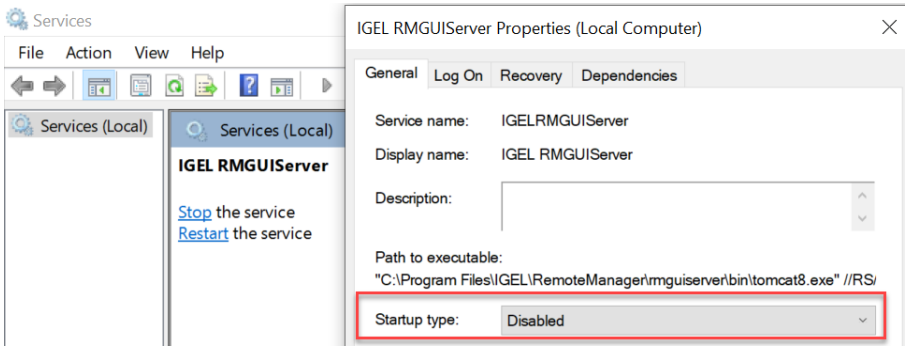
1. Wenn die Geräte die UMS über die IP-Adresse finden, können sie sich nur dann mit dem neuen Server verbinden, wenn die IP-Adresse des neuen Servers vor der Migration erstellt wird. So legen Sie die IP-Adresse fest:

   a. Erstellen Sie ein OS 11- und ein OS 12-Profil mit der neuen UMS-Server-IP. Der neue Server muss unter **System > Remote Management** aufgeführt werden. Weitere Informationen finden Sie unter Fernadministration und Remote Management.

   b. Weisen Sie die Profile zu.

   c. Überprüfen Sie, ob alle Geräte ihre Einstellungen erhalten haben, indem Sie unter **Views** eine Ansicht mit dem Kriterium Last Boot Time erstellen. Weitere Informationen finden Sie unter Wie erstelle ich eine neue View in der IGEL UMS?.

2. Stoppen Sie den Dienst `IGEL RMGUIServer` (siehe IGEL UMS HA-Dienste und -Prozesse (see page 949) für Anweisungen) und setzen Sie den Starttyp auf "Deaktiviert", um einen zufälligen Parallelbetrieb mit dem neuen UMS Server zu verhindern.



3. Erstellen Sie ein Backup unter **UMS Administrator > Backups** und kopieren Sie es auf ein Speichermedium. Nehmen Sie alle Optionen in das Backup auf. Detaillierte Anweisungen finden Sie im Abschnitt "Embedded-Datenbank" unter Ein Backup der IGEL UMS erstellen (see page 720).

   Das Backup der **Serverkonfigurationen** enthält die meisten Konfigurationen des Bereichs Einstellungen (see page 709) im UMS Administrator. Ausnahmen: **Web-Serverport**, **JWS-Serverport** und **Ciphers** – sie sind hostspezifisch, d.h. sie werden auf jedem Server separat gespeichert und können nicht Teil eines Backups sein. Daher sollten Sie die Werte dieser Einstellungen notieren, wenn sie vom Standard abweichen, und im Falle eines Recovery-/Migrationsverfahrens müssen sie auf jedem Server manuell angepasst werden.

4. Erstellen Sie ein Backup der UMS-ID im **UMS Administrator > UMS-ID-Backup**. Detaillierte Anweisungen finden Sie unter Übertragen oder Registrieren der UMS-ID (see page 101).

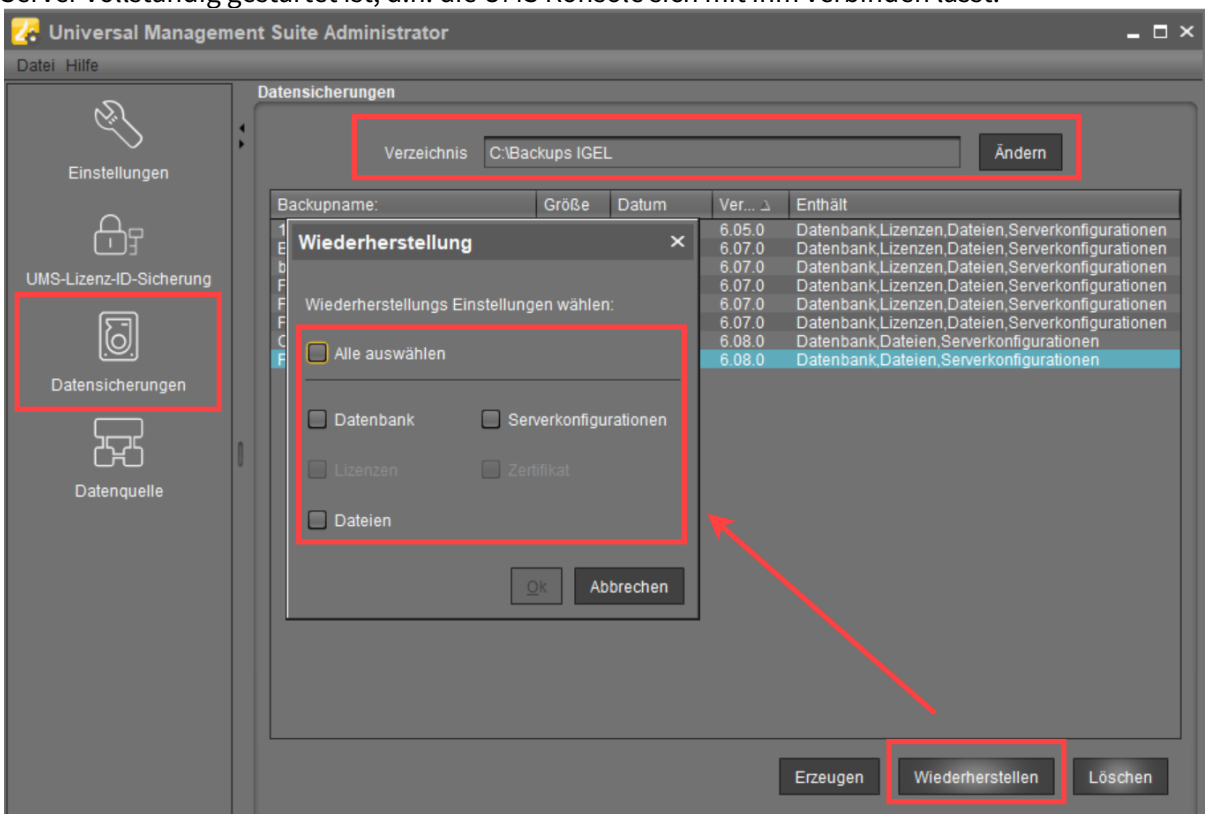
5. Erstellen Sie eine Backup aller Dateien im folgenden Ordner. (Sie müssen sie auf dem neuen Server wiederherstellen.)
   `[IGEL Installationsverzeichnis]/rmguiserver/webapps/ums_filetransfer`

6. Gehen Sie in der UMS Konsole zu **UMS Administration > UMS Netzwerk > Server** und notieren Sie sich die Prozess-ID des UMS Servers.

Auf dem neuen Server

1. Installieren Sie die UMS auf dem neuen Server. Verwenden Sie nach Möglichkeit denselben Benutzer und dasselbe Passwort für die Datenbank. Die Installationsanweisungen finden Sie unter IGEL UMS Installation (see page 246).

2. Wählen Sie unter **UMS Administrator > Datensicherungen** das Verzeichnis mit Ihrem Backup und stellen Sie die entsprechende Backupdatei mit allen Optionen wieder her. Warten Sie, bis der UMS Server vollständig gestartet ist, d.h. die UMS Konsole sich mit ihm verbinden lässt.



3. Übertragen Sie die UMS-ID der vorherigen UMS Installation auf den neuen Server: **UMS Administrator > UMS-ID-Sicherung > Wiederherstellen**. Alternativ können Sie auch die neue UMS-ID registrieren, die bei der Installation des neuen Servers erstellt wurde. Detaillierte Anweisungen finden Sie unter Übertragen oder Registrieren der UMS-ID (see page 101).

   ⚠ Es wird empfohlen, die gleiche UMS-ID zu verwenden. Die Verbindung zu ILP, App Portal und anderen Diensten ist von der UMS-ID abhängig und würde bei einer Änderung beeinträchtigt werden.

4. Übertragen Sie ggf. hostspezifische Serverkonfigurationen auf den neuen Server.

5. Stellen Sie die Dateien im Ordner `[IGEL Installationsverzeichnis]/rmguiserver/webapps/ums_filetransfer` wieder her, wobei Sie die Ordnerstruktur des alten Servers beibehalten.

6. Falls ICG verwendet wird: Verbinden Sie die bereits vorhandenen ICGs wie unter ICG-Verbindung nach der UMS Server-Migration oder -Neuinstallation mit der gleichen Datenbank (see page 118) beschrieben.

7. Starten Sie den Dienst `IGEL RMGUIServer` neu. Wenn die Geräte die UMS über die IP-Adresse finden, sollten sie sich automatisch verbinden.

8. Wenn die Geräte die UMS über DNS/DHCP finden:
   a. Passen Sie das DHCP-Tag und den DNS-Alias `igelrmserver` mit der IP oder FQDN des neuen UMS Servers an. Siehe Geräte automatisch an der IGEL UMS registrieren (see page 337).

      ⓘ Die Konfiguration des DHCP-Tags und des DNS-Alias ist keine Einstellung, die innerhalb der IGEL Software vorgenommen werden kann. Diese müssen Sie innerhalb Ihrer individuellen Netzwerkumgebung auf den entsprechenden DHCP- und DNS-Servern konfigurieren.

   b. Weisen Sie den neuen Server dem alten Serverzertifikat zu oder erstellen und weisen Sie ein neues Zertifikat mit dem FQDN des neuen Servers zu. Weitere Informationen finden Sie unter Geräte automatisch an der IGEL UMS registrieren (see page 337).

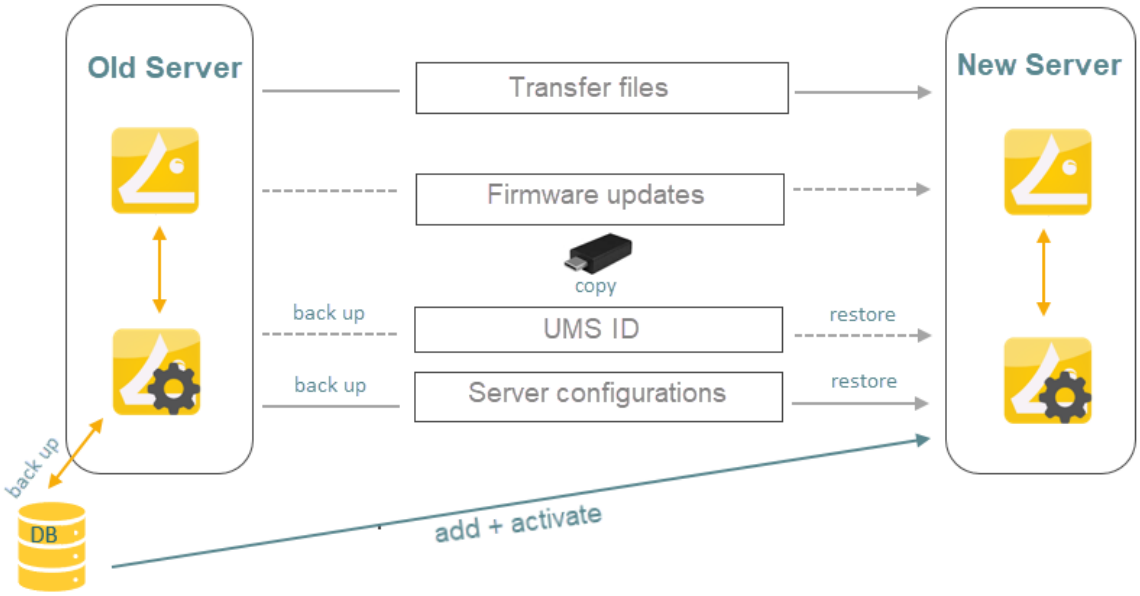
9. Öffnen Sie anschließend die UMS Konsole und prüfen Sie unter **UMS Administration > UMS Netzwerk > Server**, ob unter den aufgelisteten Komponenten ein Eintrag für den bisherigen UMS Server vorhanden ist. Ist dies der Fall, markieren Sie den Eintrag und klicken Sie im Kontextmenü auf **Löschen**.

Migration eines UMS Server mit der selben externen Datenbank

Anwendungsfall

Sie haben eine UMS Installation mit einer externen Datenbank und möchten auf einen neuen UMS Server mit der gleichen externen Datenbank migrieren.

Allgemeiner Überblick



Das Migrationsverfahren umfasst im Allgemeinen die folgenden Schritte:

1. Profil mit der IP des neuen Servers für die Fernadministration erstellen (nur notwendig, wenn Geräte die UMS über IP finden)
2. `IGEL RMGUIServer` -Dienst auf dem alten Server stoppen
3. Ein Backup des alten Servers erstellen. Checkliste für die Backups:
   - ✅ **Datenbank**
   - ✅ **Dateien**
   - ✅ **Serverkonfigurationen** (hostspezifische Serverkonfigurationen, die von den Standardeinstellungen abweichen, sind separat notiert)
   - ✅ **Firmwareupdates**
   - ✅ **UMS-ID** (siehe Übertragen oder Registrieren der UMS-ID (see page 101))
4. Hinzufügen der bestehenden externen Datenbank als Datenquelle für den neuen Server
5. Aktivieren der Datenquelle
6. Die erstellten Backups auf den neuen Server übertragen
7. DHCP-Tag und DNS-Alias auf dem neuen Server anpassen (nur erforderlich, wenn Geräte das UMS über DNS/DHCP finden)

Anweisungen

Auf dem alten Server

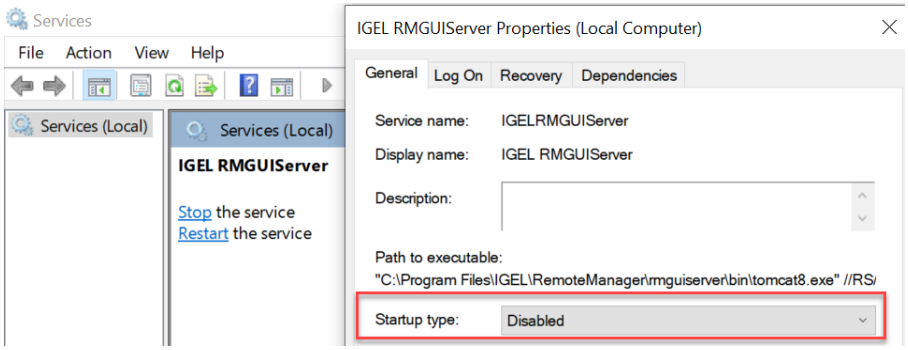
1. Wenn die Geräte die UMS über die IP-Adresse finden, können sie sich nur dann mit dem neuen Server verbinden, wenn die IP-Adresse des neuen Servers vor der Migration erstellt wird. So legen Sie die IP-Adresse fest:

    a. Erstellen Sie ein OS 11- und ein OS 12-Profil mit der neuen UMS-Server-IP. Der neue Server muss unter **System > Remote Management** aufgeführt werden. Weitere Informationen finden Sie unter Remote Management und Remote Management.

    b. Weisen Sie die Profile zu.

    c. Überprüfen Sie, ob alle Geräte ihre Einstellungen erhalten haben, indem Sie unter **Views** eine Ansicht mit dem Kriterium Last Boot Time erstellen. Weitere Informationen finden Sie unter How to Create a New View in the IGEL UMS.

2. Stoppen Sie den Dienst `IGEL RMGUIServer` (siehe IGEL UMS HA-Dienste und -Prozesse (see page 949) für Anweisungen) und setzen Sie den Starttyp auf "Deaktiviert", um einen zufälligen Parallelbetrieb mit dem neuen UMS Server zu verhindern.



3. Erstellen Sie vor der Migration die Backups, wie im Abschnitt "Externe Datenbank" unter Ein Backup der IGEL UMS erstellen (see page 720) beschrieben.

4. Notieren Sie die Werte der hostspezifischen Servereinstellungen (Webserver-Port, JWS-Server-Port und Chiffren).

5. Erstellen Sie ein Backup der UMS-ID im **UMS Administrator > UMS-ID-Backup**. Detaillierte Anweisungen finden Sie unter Übertragen oder Registrieren der UMS-ID (see page 101).

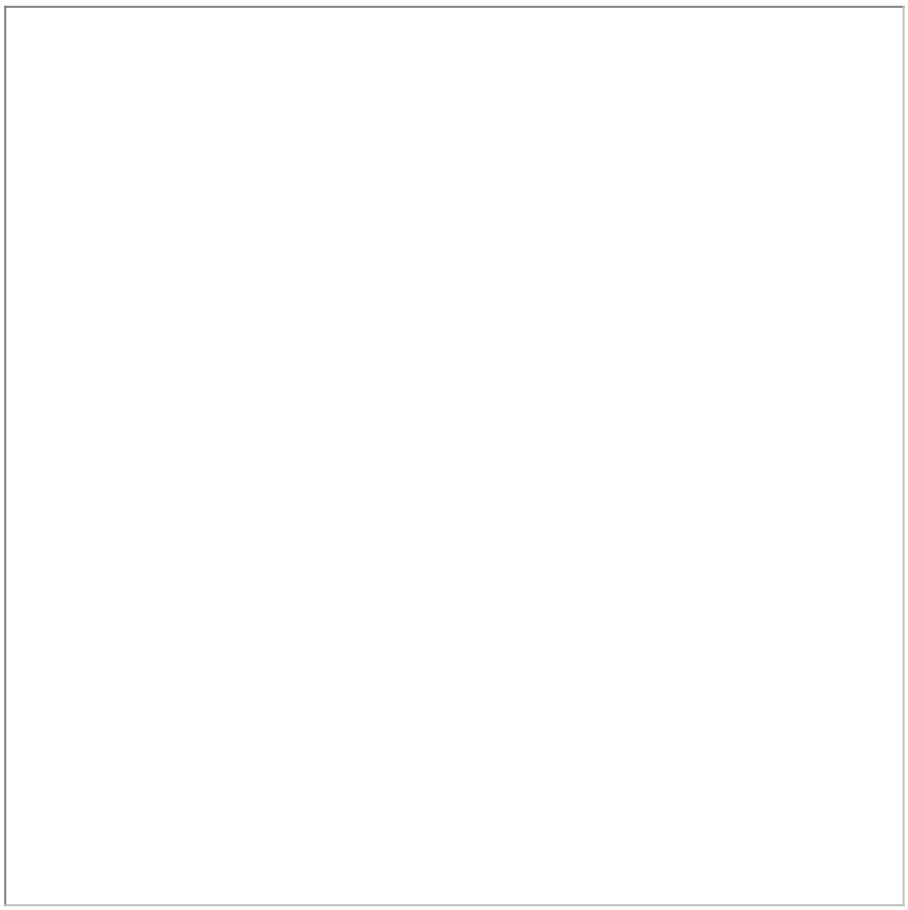
6. Erstellen Sie eine Backup aller Dateien im folgenden Ordner. (Sie müssen sie auf dem neuen Server wiederherstellen.)
   `[IGEL Installationsverzeichnis]/rmguiserver/webapps/ums_filetransfer`

7. Gehen Sie in der UMS Konsole zu **UMS Administration > UMS Netzwerk > Server** und notieren Sie sich die Prozess-ID des UMS Servers.

Auf dem neuen Server

1. Installieren Sie die UMS auf dem neuen Server. Die Installationsanweisungen finden Sie unter IGEL UMS Installation (see page 246).

2. Gehen Sie auf **UMS Administrator > Datenquelle > Neu** und geben Sie die Verbindungsangaben der vorhandenen Datenbank ein.



3. **Aktivieren** Sie die Datenquelle. Warten Sie, bis der UMS Server vollständig gestartet ist, d.h. die UMS Konsole sich mit ihm verbinden lässt.

4. Stellen Sie unter **UMS Administrator > Backups** das Backup der Serverkonfigurationen wieder her. Übertragen Sie ggf. hostspezifische Serverkonfigurationen (see page 721) auf den neuen Server.

5. Übertragen Sie die UMS-ID der vorherigen UMS Installation auf den neuen Server: **UMS Administrator > UMS-ID-Sicherung > Wiederherstellen**. Alternativ können Sie auch die neue

UMS-ID registrieren, die bei der Installation des neuen Servers erstellt wurde. Detaillierte Anweisungen finden Sie unter Übertragen oder Registrieren der UMS-ID (see page 101).

> ⚠ Es wird empfohlen, die gleiche UMS-ID zu verwenden. Die Verbindung zu ILP, App Portal und anderen Diensten ist von der UMS-ID abhängig und würde bei einer Änderung beeinträchtigt werden.

6. Stellen Sie die Dateien im Ordner `[IGEL Installationsverzeichnis]/rmguiserver/webapps/ums_filetransfer` wieder her, wobei Sie die Ordnerstruktur des alten Servers beibehalten.

7. Falls ICG verwendet wird: Verbinden Sie die bereits vorhandenen ICGs wie unter ICG-Verbindung nach der UMS Server-Migration oder -Neuinstallation mit der gleichen Datenbank (see page 118) beschrieben.

8. Starten Sie den Dienst `IGEL RMGUIServer` neu. Wenn die Geräte die UMS über die IP-Adresse finden, sollten sie sich automatisch verbinden.

9. Wenn die Geräte die UMS über DNS/DHCP finden:
   a. Passen Sie das DHCP-Tag und den DNS-Alias `igelrmserver` mit der IP oder FQDN des neuen UMS Servers an. Siehe Geräte automatisch an der IGEL UMS registrieren (see page 337).

   > ⓘ Die Konfiguration des DHCP-Tags und des DNS-Alias ist keine Einstellung, die innerhalb der IGEL Software vorgenommen werden kann. Diese müssen Sie innerhalb Ihrer individuellen Netzwerkumgebung auf den entsprechenden DHCP- und DNS-Servern konfigurieren.

   b. Weisen Sie den neuen Server dem alten Serverzertifikat zu oder erstellen und weisen Sie ein neues Zertifikat mit dem FQDN des neuen Servers zu. Weitere Informationen finden Sie unter Geräte automatisch an der IGEL UMS registrieren (see page 337).

10. Nur für HA-Installationen: Aktualisieren Sie die Hostzuweisung für die Aufgabenausführung. Anweisungen finden Sie unter Hostzuweisung für die Aufgabenausführung aktualisieren (see page 104).

11. Öffnen Sie anschließend die UMS Konsole und prüfen Sie unter **UMS Administration > UMS Netzwerk > Server**, ob unter den aufgelisteten Komponenten ein Eintrag für den bisherigen UMS Server vorhanden ist. Ist dies der Fall, markieren Sie den Eintrag und klicken Sie im Kontextmenü auf **Löschen**.

Mit einer anderen Datenbank

Wenn Sie auf einen neuen UMS Server migrieren und gleichzeitig Ihre Daten in eine andere Datenbank übertragen wollen, finden Sie hier die Anleitung.

Datenübertragung

Vor der Migration müssen Sie die UMS-Daten in die neue Datenbank übertragen:

1. Öffnen Sie den IGEL UMS Administrator des aktuellen Servers.
2. Klicken Sie im UMS Administrator des aktuellen Servers auf **Datenquelle > Neu**, um eine Datenquelle für die neue Datenbank einzurichten, die Sie verwenden möchten.
3. Klicken Sie **Kopieren**, um die alte Datenquelle in die neue zu kopieren.
4. Aktivieren Sie die neue Datenquelle.
5. Warten Sie, bis der UMS Server vollständig gestartet ist, d.h. die UMS Konsole sich mit ihm verbinden kann.

> Weitere Informationen zur Verwaltung von Datenquellen im IGEL UMS Administrator finden Sie unter Datenquelle (see page 729).

Migration

Nach der Übertragung der Daten können Sie die Migration auf der Grundlage der Datenbank beginnen:

- Wenn die neue Datenquelle eine eingebettete Datenbank ist, befolgen Sie die Anweisungen in UMS mit derselben Embedded-Datenbank (see page 92).
- Wenn die neue Datenquelle eine externe Datenbank ist, befolgen Sie die Anweisungen in UMS mit der selben externen Datenbank (see page 96).

Übertragen oder Registrieren der UMS-ID

Es gibt zwei verschiedene Möglichkeiten, mit der UMS-ID (see page 639) zu verfahren, wenn Sie den UMS Server migrieren:

- Die UMS-ID übertragen (see page 101): Bei dieser Methode erstellen Sie ein Backup der alten UMS-ID und nehmen es mit. Die UMS-ID, die bei der Installation des neuen UMS Servers automatisch erstellt wird, wird überschrieben.
  Der Vorteil: Sie müssen die Lizenzpakete im ILP nicht neu zuordnen.
- Die neue UMS-ID registrieren (see page 102): Bei dieser Methode registrieren Sie die UMS-ID des neuen Servers im IGEL Lizenz-Portal.
  Vorteil: Sie brauchen die UMS-ID des alten Servers nicht zu kennen.
  Nachteil: Um Ihre UMS bei den IGEL Cloud Services zu authentifizieren, müssen Sie Ihre UMS mit der neuen UMS-ID erneut registrieren.

Die UMS-ID übertragen

Alter Server: Erstellen Sie ein Backup der UMS-ID

1. Öffnen Sie den UMS Administrator auf Ihrem alten Server.

   > Standardpfad zum UMS Administrator:
   > Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
   > Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
   > Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

2. Gehen Sie zu **UMS-ID-Sicherung** und erstellen Sie ein Backup wie unter UMS-ID-Sicherung im IGEL Administrator (see page 713) beschrieben.
3. Gehen Sie in Ihrem Datei-Explorer zum angegebenen Ordner, in dem Sie das UMS-ID-Backup gespeichert haben.
4. Kopieren Sie das Backup (z.B. `UMS ID_backup before migration.ksbak`) in ein Verzeichnis Ihrer neuen UMS-Server-Umgebung.

Neuer Server: Stellen Sie die UMS-ID auf dem neuen Server wieder her

1. Öffnen Sie den UMS Administrator auf dem neuen Server.
2. Gehen Sie zu **UMS-ID-Sicherung** und stellen Sie das Backup wieder her, wie unter UMS-ID-Sicherung im IGEL Administrator (see page 713) beschrieben.

   Die UMS-ID ist nun in der neuen UMS-Umgebung gespeichert.

Die neue UMS-ID registrieren

Im IGEL Lizenz-Portal (ILP)

1. Melden Sie sich im IGEL Lizenz-Portal (ILP) unter https://activation.igel.com an. Wenn Sie sich noch nicht registriert haben, müssen Sie dies als Erstes machen.
   Das Dashboard wird angezeigt.

2. Wählen Sie **UMS-ID**.
   Die Seite **UMS-ID** wird angezeigt.

3. Klicken Sie **UMS-ID registrieren**.
   Der Dialog **UMS-ID registrieren** öffnet sich.

4. Geben Sie in das Feld **UMS-ID-Name** den Namen für die UMS-ID ein.

5. Laden Sie die Zertifikat-Datei, die Sie von der UMS exportiert haben, hoch (siehe UMS ID erhalten) und klicken Sie **Ok**.
   Die UMS-ID wurde registriert. Wenn das die erste registrierte UMS-ID ist oder wenn Sie es einfach als Standard UMS-ID definiert haben, wird der Dialog **Lose Product Packs zuweisen** angezeigt.

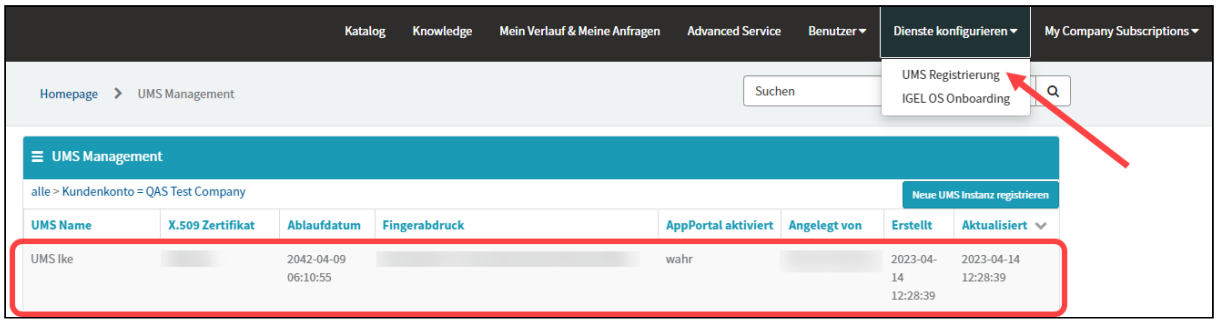
6. Wenn der Dialog **Lose Product Packs zuweisen** angezeigt wird, klicken Sie **Ok**, um Product Packs zuzuweisen, und fahren Sie mit Product Pack zur UMS-ID zuweisen fort.

Eine detaillierte Anleitung mit Screenshots finden Sie unter Registering Your UMS Licensing ID.

Im IGEL Customer Portal

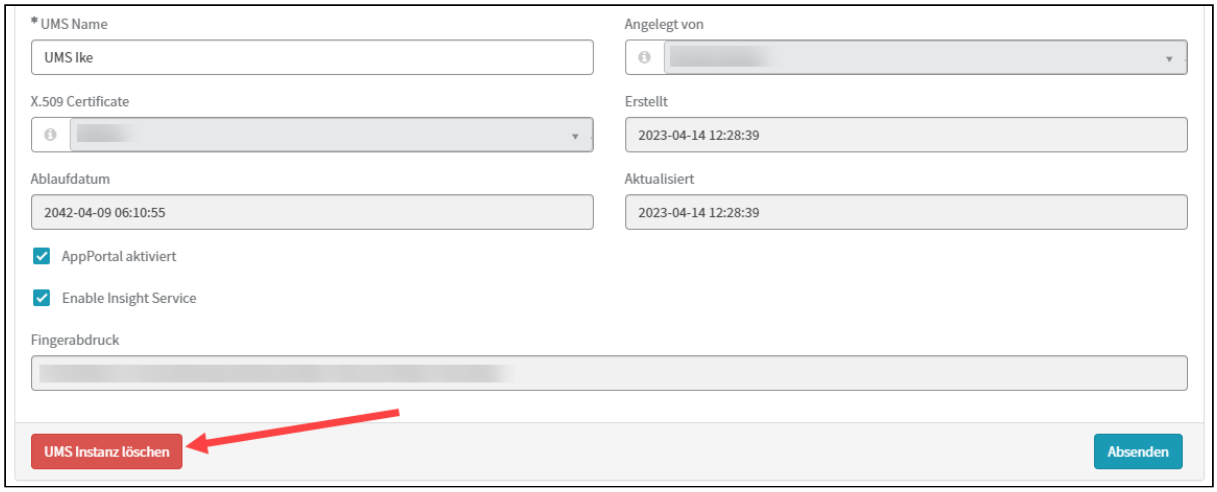
1. Melden Sie sich beim IGEL Customer Portal[3] an.

2. Gehen Sie zu **Dienste konfigurieren > UMS Registrierung** und wählen Sie Ihre alte UMS Instanz aus.



3 https://cosmos.igel.com/

3. Klicken Sie **UMS Instanz löschen**.



> ⚠ Wenn Sie Ihre UMS Instanz löschen, können Sie keine Apps in die UMS importieren oder das lokale App Portal auf den IGEL OS 12-Geräten öffnen.

4. Registrieren Sie Ihre UMS neu, wie unter Registrierung der IGEL Universal Management Suite (UMS) beschrieben.

Hostzuweisung für die Aufgabenausführung aktualisieren

Die Aufgabenausführung in der UMS verwendet eine Zuordnung von Geräten zu UMS Servern, um zu vermeiden, dass ein Job mehrfach auf demselben Gerät ausgeführt wird. Wenn ein UMS Server migriert wird, muss dieses Mapping angepasst werden.

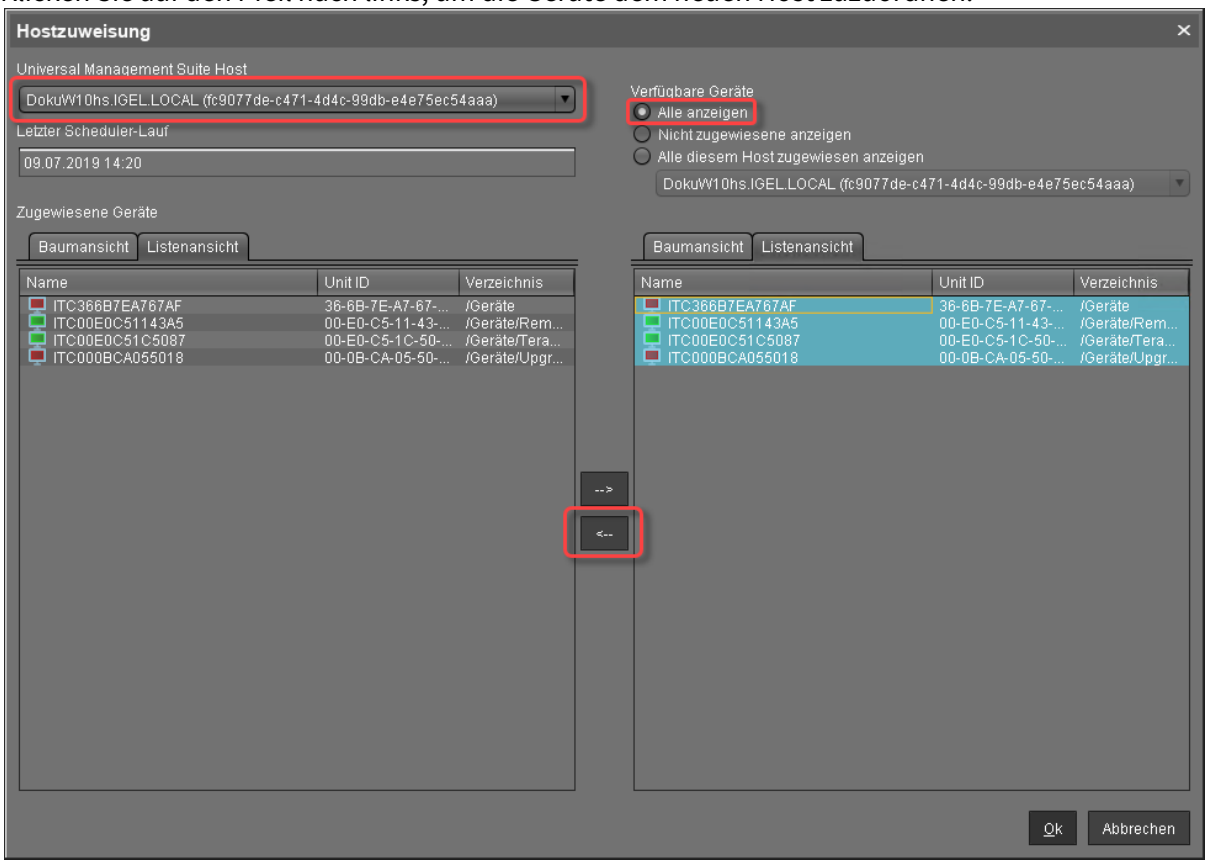
> Das Mapping ist nur für High Availability (HA)- und Distributed UMS-Installationen relevant. Bei Standardinstallationen (Einzelinstanz) müssen die Hostzuordnungen nicht angepasst werden. In HA- und Distributed UMS-Installationen führen Sie bitte die folgenden Schritte aus.

1. In der UMS Konsole des neuen Servers gehen Sie auf **UMS Administration > UMS Netzwerk > Server > [neuer Server]**.
2. Finden Sie die Prozess-ID des neuen Servers.

3. Wählen Sie in der Menüleiste der UMS Konsole **Extras > Geplante Aufgaben > Hostzuweisung**.
4. Wählen Sie den neuen Server und überprüfen Sie die Prozess-ID.
5. Aktivieren Sie unter **Verfügbare Geräte** die Option **Alle anzeigen**.
6. Wählen Sie in der **Listenansicht** auf der rechten Seite alle Geräte aus.

   > Um alle Geräte auszuwählen, setzen Sie den Fokus auf de Liste und drücken Sie [Strg+a].

7. Klicken Sie auf den Pfeil nach links, um die Geräte dem neuen Host zuzuordnen.



UMS Datenbank von der Embedded-Datenbank auf Microsoft SQL Server migrieren

Dieses Dokument beschreibt die Migration der Datenbank einer Universal Management Suite (UMS) Installation von Embedded-DB auf einen Microsoft SQL Server.

Hierbei handelt es sich um eine beispielhafte Darstellung. Wenn sie umgekehrt mirgrieren möchten oder andere Datenbanken mirgrieren möchte, laufen immer dieselben Schritte ab. Sie können sich immer an dieser Beschreibung orientieren.

IGEL Demo Kanal

Einrichten der SQL-Datenbank

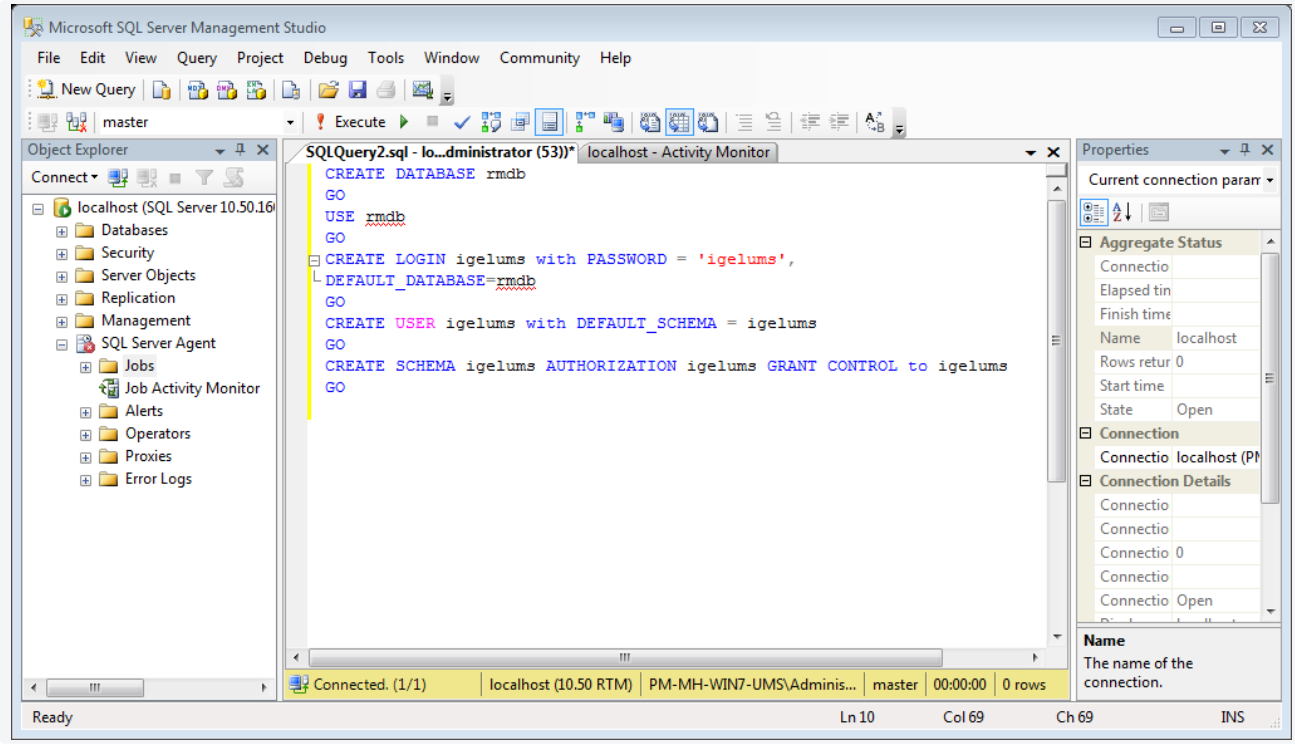
> ⚠ Die UMS unterstützt nur die Standardsortierungen von Microsoft SQL Server, die Groß- und Kleinschreibung nicht unterscheiden ("CI", case insensitive). Stellen Sie daher sicher, dass der Parameter **Sortierung** in MS SQL Server richtig gesetzt ist.

▶ Führen Sie das folgende SQL-Skript auf dem Microsoft SQL Server aus, um Datenbank, Login, Benutzer und Schema zu erstellen. Ersetzen Sie die Platzhalter wie z. B. `[Databasename]` durch Einstellungen Ihrer Wahl.

`[sql-user]` kann ein SQL Konto oder ein Microsoft Active Directory (AD) Konto sein; weitere Informationen zu Letzterem finden Sie unter UMS mit einem SQL Server über Active Directory verbinden. Das Skript verwendet den gleichen String für Login, Benutzer und Schema, um die UMS Einrichtung zu vereinfachen.

> ⓘ Für den **Benutzernamen** für die externe Datenbank gelten folgende Regeln:
> - Er besteht nur aus **Kleinbuchstaben** oder aus **Großbuchstaben**.
> - Das einzig erlaubte Sonderzeichen ist der **Tiefstrich** ("_").
>
> Groß- und Kleinbuchstaben dürfen nicht gemischt werden.
> Verwenden sie keine Punkte, Leerzeichen, kein Minus oder @-Zeichen.

```
CREATE DATABASE [databasename]
GO
USE [databasename]
GO
CREATE LOGIN [sql-user] with PASSWORD = '[password]',
DEFAULT_DATABASE=[databasename]
GO
CREATE USER [sql-user] with DEFAULT_SCHEMA = [sql-user]
GO
CREATE SCHEMA [sql-user] AUTHORIZATION [sql-user] GRANT CONTROL to [sql-user]
GO
```

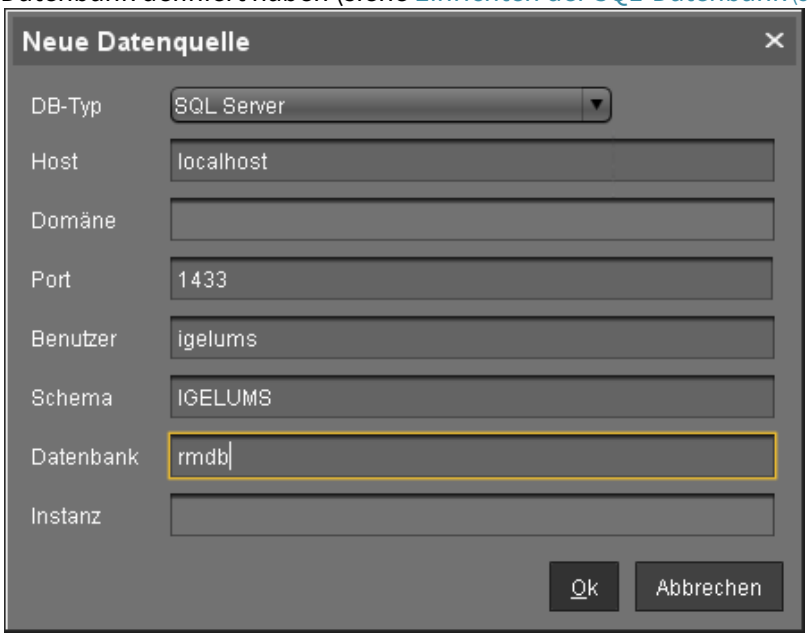

Microsoft SQL Server Management Studio
File Edit View Query Project Debug Tools Window Community Help
New Query
master
Execute
Object Explorer
Connect
localhost (SQL Server 10.50.16
Databases
Security
Server Objects
Replication
Management
SQL Server Agent
Jobs
Job Activity Monitor
Alerts
Operators
Proxies
Error Logs
SQLQuery2.sql - lo...dministrator (53))*
localhost - Activity Monitor
CREATE DATABASE rmdb
GO
USE rmdb
GO
CREATE LOGIN igelums with PASSWORD = 'igelums',
DEFAULT_DATABASE=rmdb
GO
CREATE USER igelums with DEFAULT_SCHEMA = igelums
GO
CREATE SCHEMA igelums AUTHORIZATION igelums GRANT CONTROL to igelums
GO
Properties
Current connection param
Aggregate Status
Connectio
Elapsed tin
Finish time
Name localhost
Rows retur 0
Start time
State Open
Connection
Connectio localhost (PM
Connection Details
Connectio
Connectio
Connectio 0
Connectio
Connectio Open
Name
The name of the connection.
Connected. (1/1)
localhost (10.50 RTM)
PM-MH-WIN7-UMS\Adminis...
master
00:00:00
0 rows
Ready
Ln 10
Col 69
Ch 69
INS

Kopieren von Datenbankinhalten

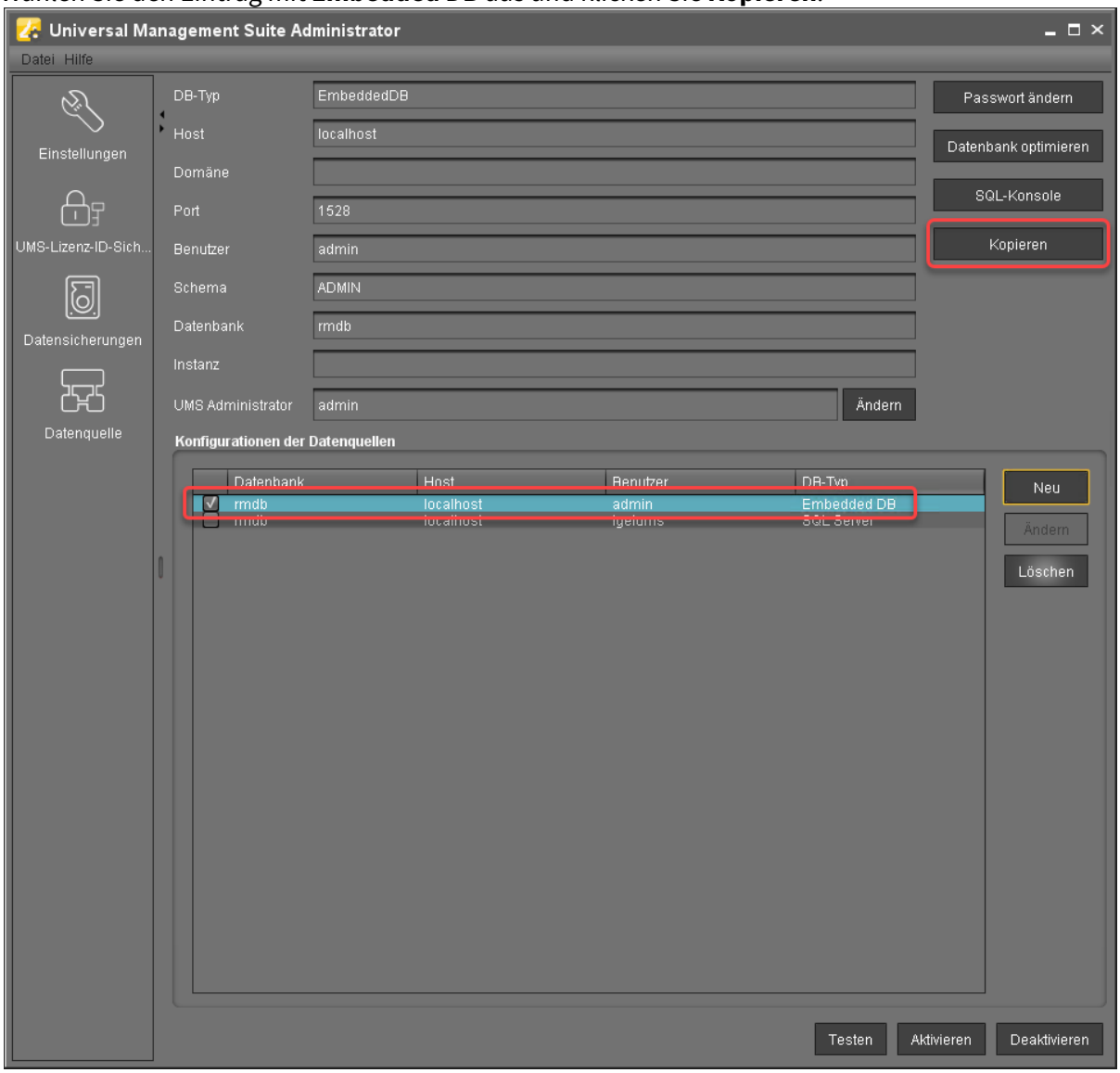
1. Starten Sie den IGEL Universal Management Suite Administrator.

   > Standardpfad zum UMS Administrator:
   > Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
   > Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
   > Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

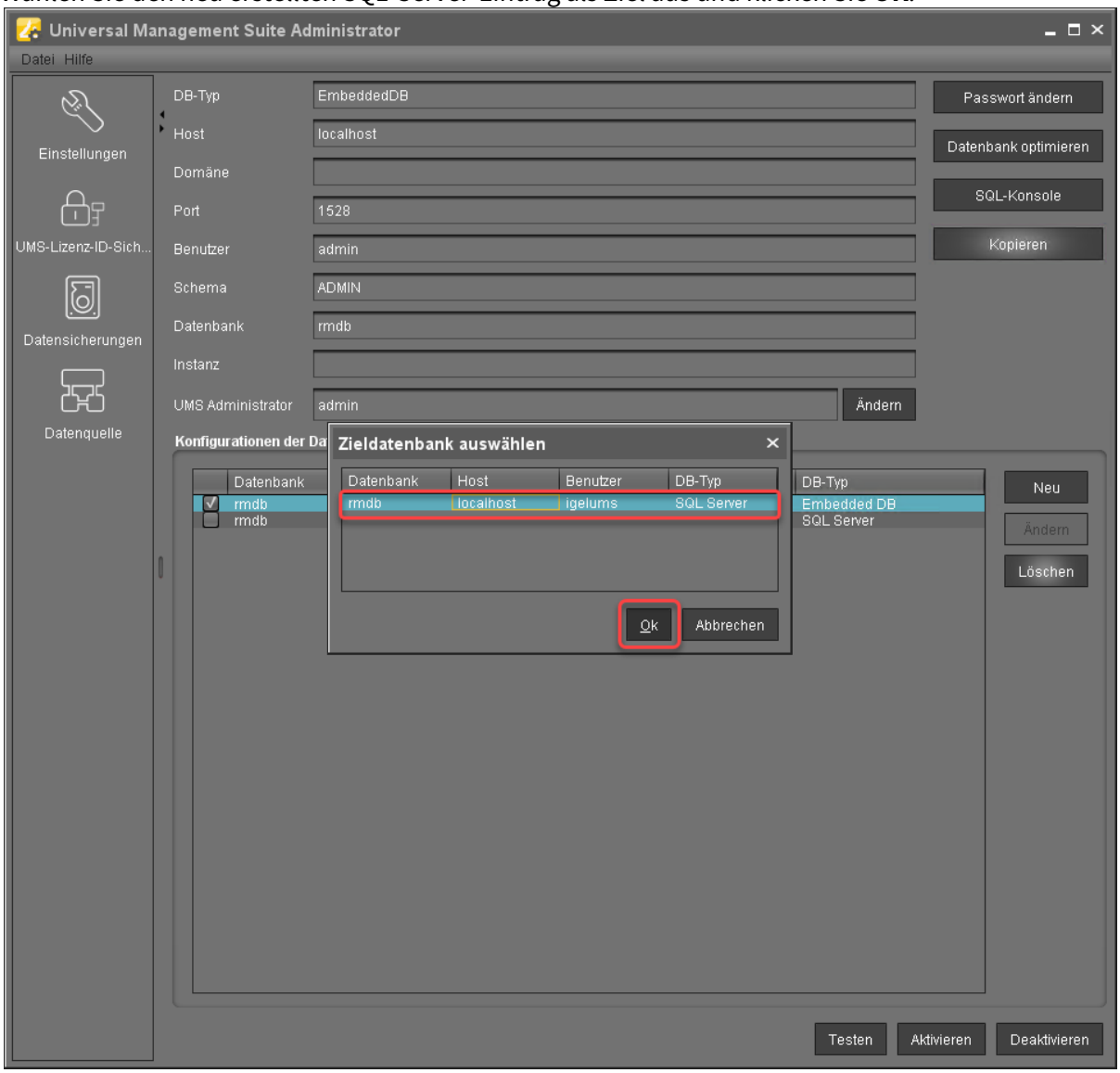
2. Gehen Sie auf **Datenquelle > Neu**, um eine neue SQL Server-Datenquelle zu erstellen; verwenden Sie genau den Datenbanknamen und die Einstellungen, die Sie beim Aufsetzen der SQL-Datenbank definiert haben (siehe Einrichten der SQL-Datenbank (see page 107)).



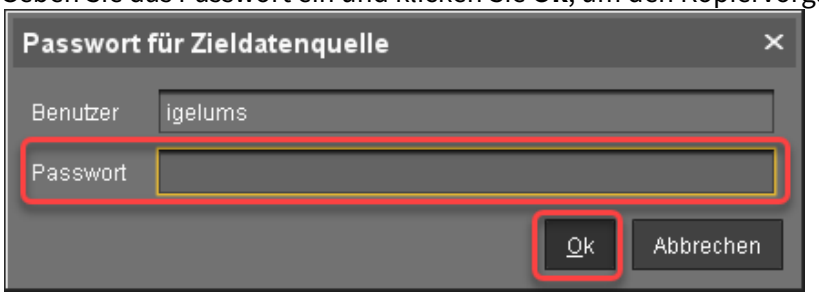
3. Wählen Sie den Eintrag mit **Embedded DB** aus und klicken Sie **Kopieren**.



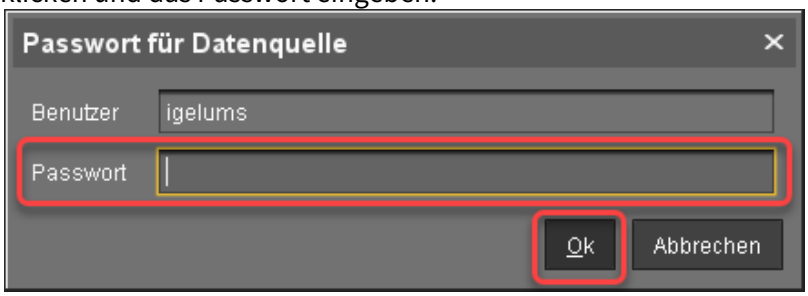
4. Wählen Sie den neu erstellten SQL-Server-Eintrag als Ziel aus und klicken Sie **OK**.



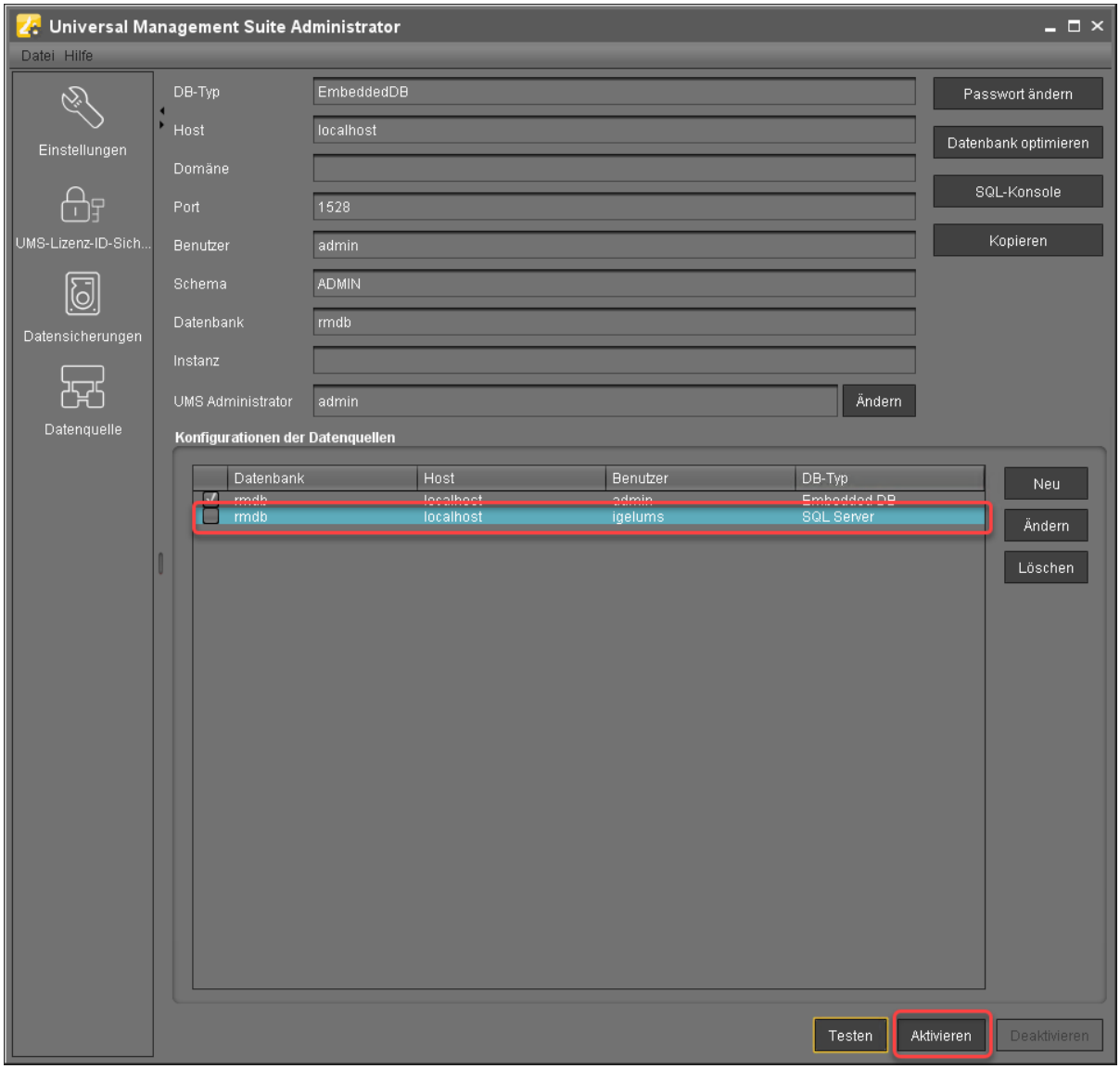
5. Geben Sie das Passwort ein und klicken Sie **Ok**, um den Kopiervorgang zu starten.



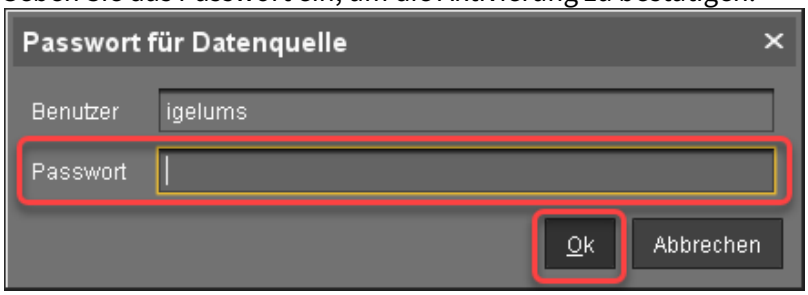
6. Wenn der Kopiervorgang beendet ist, testen Sie die Datenbankverbindung, indem Sie auf **Test** klicken und das Passwort eingeben.



7. Wenn der Test erfolgreich war, wählen Sie die **SQL Server**-Datenquelle aus und klicken Sie **Aktivieren**.



8. Geben Sie das Passwort ein, um die Aktivierung zu bestätigen.



Nun ist der Microsoft SQL Server als Datenquelle eingerichtet. Sichern Sie von nun an den SQL Server, um UMS Daten zu sichern.

Auf die gleiche Weise können Sie bei Bedarf auf die Embedded-Datenbank zurückgreifen.

Beschädigte UMS Embedded-DB wiederherstellen

Umgebungsbedingungen

- UMS 6 auf Windows oder Linux

Wenn die Embedded-Datenbank einer UMS* beschädigt ist, versuchen Sie die folgenden Maßnahmen, um das Problem zu beheben.

*Die zugrunde liegende Technologie der eingebetteten Datenbank ist Apache Derby.

Eine mit dem UMS Administrator erstellte Datenbanksicherung wiederherstellen

Wenn ein Backup der Embedded-Datenbank verfügbar ist (siehe Ein Backup der IGEL UMS erstellen (see page 720)), stellen Sie das Backup wieder her, sehen Sie Backup wiederherstellen (see page 725).

Wiederherstellen einer dateibasierten Sicherung

Wenn eine unverfälschte Kopie der Datenbankdateien unter `C:\Program Files...\IGEL\RemoteManager\db\rmdb` (Standardinstallationspfad unter Windows) und/oder `/opt/IGEL/RemoteManager/db/rmdb/` (Standardinstallationspfad unter Linux) verfügbar ist, können Sie die Dateikopie wiederherstellen. Im weiteren Verlauf dieser Anleitung werden die oben genannten möglichen Pfade als `RMDB_PATH` bezeichnet.

Um das Backup wiederherzustellen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie den UMS Administrator und gehen Sie auf **Datenquelle** im Menü links.

   > Standardpfad zum UMS Administrator:
   > Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
   > Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
   > Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

2. Löschen Sie im Bereich **Datenquelle** die beschädigte Derby DB.
3. Erstellen Sie eine neue Embedded-DB mit genau dem gleichen Benutzernamen und Passwort, das Sie für die gelöschte DB verwendet haben.
4. Deaktivieren Sie die neu erstellte DB.
5. Stoppen Sie den UMS Server-Dienst. Details dazu, wie Sie ihn stoppen können, finden Sie unter IGEL UMS HA-Dienste und -Prozesse (see page 949).
6. Löschen Sie alle Dateien, die sich im Ordner unter `RMDB_PATH` befinden.
7. Kopieren Sie Ihre zuvor gesicherten Dateien nach `RMDB_PATH.`
8. Aktivieren Sie die DB mit dem UMS Administrator unter **Datenquelle**.
9. Warten Sie 1 - 2 Minuten und melden Sie sich in der UMS Konsole an.

Disaster Recovery: UMS mit externer Datenbank

Die folgenden Anweisungen setzen ein ordnungsgemäßes Backup Ihrer Umgebung voraus, siehe den Abschnitt "Externe Datenbank" unter Ein Backup der IGEL UMS erstellen (see page 720).

Ablauf im Falle der Disaster Recovery

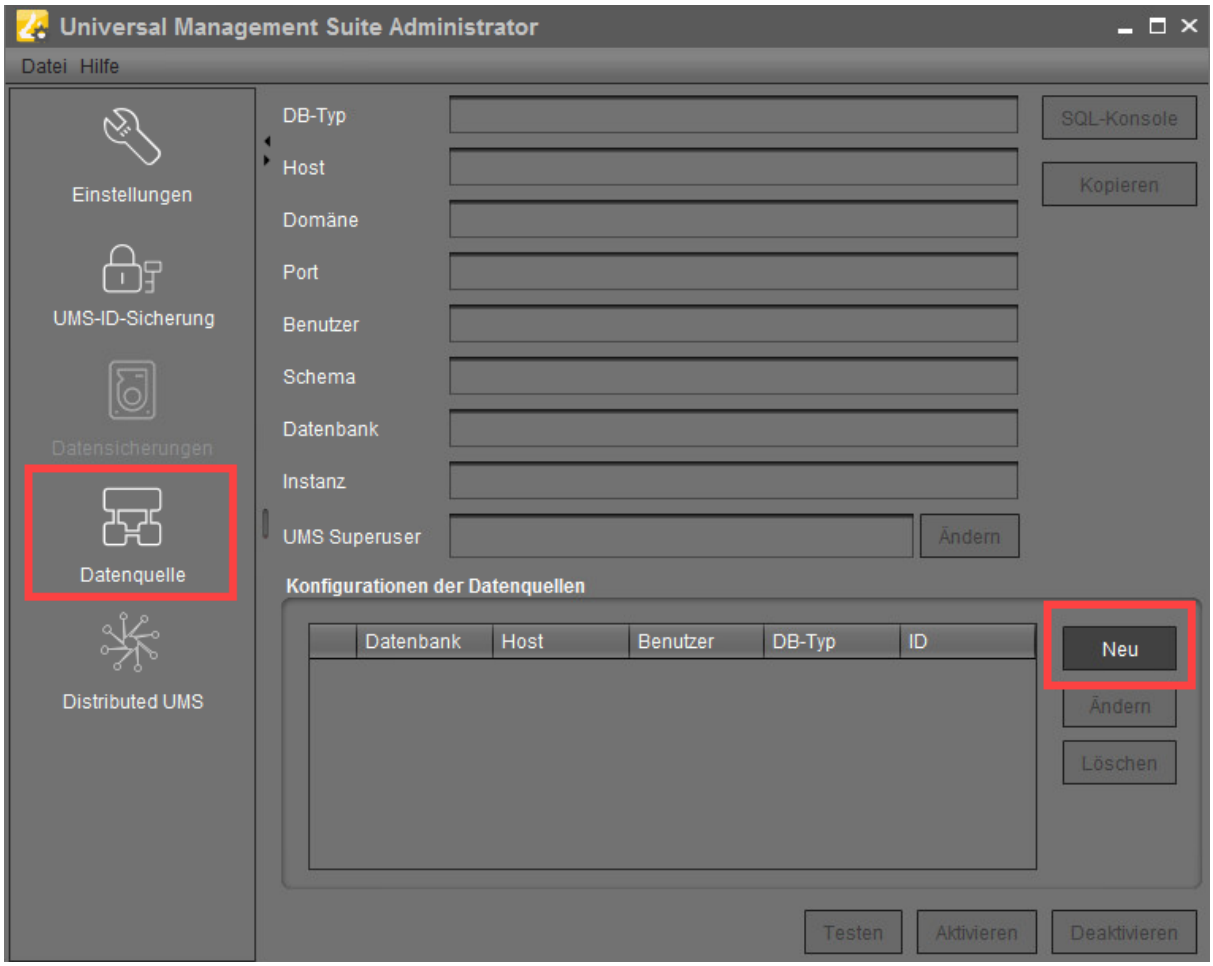
1. Installieren Sie die UMS auf dem Server, siehe IGEL UMS Installation (see page 246). Alle Komponenten der UMS müssen wie zuvor installiert werden:
   a. Die gleiche UMS Version
   b. Dieselbe Netzwerkkonfiguration des Hostrechners (dieselben IP-Adressen, Ports)
   c. Nur für HA-Installationen (High Availability) (see page 909): Verwenden Sie während der Installation das gespeicherte IGEL Netzwerktoken. Siehe den Abschnitt "Die Installation starten" unter Einem HA-Netzwerk weitere Server hinzufügen (see page 924).

2. Stoppen Sie den/die bestehenden UMS Server. Wie Sie das tun können, erfahren Sie unter IGEL UMS HA-Dienste und -Prozesse (see page 949).

3. Kopieren Sie alle gespeicherten Dateien und Firmwareupdates aus dem `[IGEL Installationsverzeichnis]/rmguiserver/webapps/ums_filetransfer` auf den/die neuen UMS Server – ohne den `WEB-INF` Ordner.
   Wenn Sie eine HA-Umgebung haben, siehe auch Welche Dateien werden automatisch zwischen den IGEL UMS Servern synchronisiert? (see page 151).

4. Stellen Sie das Datenbankbackup mit den vom DBMS-Hersteller empfohlenen Verfahren wieder her.

5. Fügen Sie die Datenbankverbindung zu Ihrer externen Datenbank auf jedem UMS Server hinzu: **UMS Administrator > Datenquelle > Neu**.



6. Klicken Sie **Aktivieren**, um die Datenquelle zu aktivieren.
   Der UMS Server wird danach automatisch gestartet.

7. Stellen Sie unter **UMS Administrator > Datensicherungen > Wiederherstellen** das Backup der Serverkonfigurationen auf jedem UMS Server wieder her. Übertragen Sie ggf. hostspezifische Serverkonfigurationen (see page 721) auf den/die neuen Server.

8. Stellen Sie unter **UMS Administrator > UMS-ID-Sicherung > Wiederherstellen** das Backup der UMS-ID wieder her.

9. Nur für HA- und Distributed UMS-Installationen: Prüfen Sie die Hostzuweisungen für die Aufgabenausführung und passen Sie sie ggf. an. Siehe Hostzuweisung für die Aufgabenausführung aktualisieren (see page 104).

ⓘ Öffnen Sie anschließend die UMS Konsole und prüfen Sie unter **UMS Administration > UMS Netzwerk > Server**, ob unter den aufgelisteten Komponenten ein Eintrag für den bisherigen UMS Server vorhanden ist. Ist dies der Fall, markieren Sie den Eintrag und klicken Sie im Kontextmenü auf **Löschen**.

Bei den HA-Installationen muss das Gleiche für die Load-Balancer gemacht werden: **UMS Administration > UMS Netzwerk > Load Balancer**.

Wenn Sie eine UMS Installation mit einer Embedded-Datenbank haben, kann der folgende Artikel von Interesse sein: Beschädigte UMS Embedded-DB wiederherstellen (see page 114).

ICG-Verbindung nach der UMS Server-Migration oder -Neuinstallation mit der gleichen Datenbank

Nachdem Sie Ihren UMS Server migriert oder mit der gleichen Datenbank neu installiert haben bzw. eine Datenbanksicherung auf diesem neu installierten Server wiederhergestellt haben, kann der Server keine Verbindung zu einem bereits vorhandenen IGEL Cloud Gateway (ICG) herstellen. Dies liegt daran, dass die ICG-Anmeldeinformationen an die alte Prozess-ID gebunden sind.

Es gibt zwei Möglichkeiten, das Problem zu lösen:

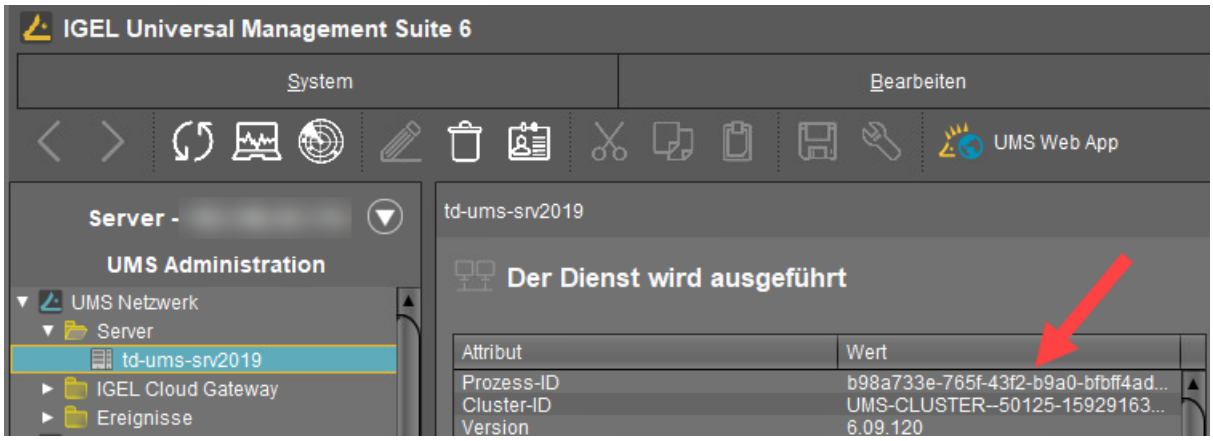
- Die Verbindung zum bestehenden ICG beibehalten (see page 118): Gilt für UMS Version 6.09.100 und höher. Bei dieser Methode befolgen Sie die unteren Anweisungen genau in der angegebenen Reihenfolge. Wichtig ist, den UMS Server NICHT neu zu starten, bevor Sie diese Schritte ausführen. Andernfalls können Sie sich nicht mit dem vorhandenen ICG verbinden und müssen es neu installieren.
- ICG-Neuinstallation (see page 120): Gilt für alle UMS Versionen. Bei dieser Methode müssen Sie das ICG deinstallieren und anschließend neu installieren.

> Mit den beiden Methoden gibt es keine negativen Auswirkungen auf Ihre Endgeräte – sie werden weiter autark arbeiten. Ausnahme: Anmeldung über Shared Workplace (SWP) (see page 951).

Die Verbindung zum bestehenden ICG beibehalten

Vor UMS 6.09.100 war es immer notwendig, die bestehenden ICGs nach der Migration des UMS Servers oder der Neuinstallation des UMS Servers mit der gleichen Datenbank (bzw. mit der Backup-Wiederherstellung) neu zu installieren. Ab UMS 6.09.100 ist es möglich, die Verbindung zum bereits existierenden ICG beizubehalten. Gehen Sie dafür wie folgt vor:

1. Öffnen Sie auf dem alten Server / vor der Reinstallation des Servers die UMS Konsole und gehen Sie zu **UMS Administration > UMS Netzwerk > Server**. Notieren Sie sich die Prozess-ID Ihres UMS Servers.

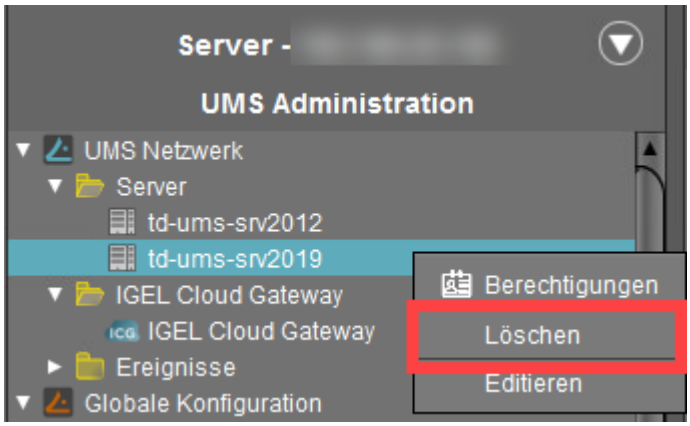


2. Installieren Sie den UMS Server. Informationen zur Installation der UMS finden Sie unter IGEL UMS Installation (see page 246).

3. Stellen Sie im UMS Administrator das Backup wieder her (siehe Backup wiederherstellen (see page 725)) oder, im Falle einer externen Datenbank, verbinden Sie die vorhandene Datenquelle und aktivieren Sie diese (siehe Wie kann ich eine Datenquelle im IGEL UMS Administrator einrichten? (see page 730)).
   Die Einträge mit der alten und der neuen Prozess-ID werden in der UMS Konsole unter **UMS Administration > UMS Netzwerk > Server** und **IGEL Cloud Gateway > [ICG-Name]** angezeigt.

4. Gehen Sie in der UMS Konsole zu **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway > [ICG-Name]** und klicken Sie auf die Schaltfläche **Verbinden**  .
   Wenn mehrere ICGs installiert sind, führen Sie dies für jedes ICG durch.
   

5. Gehen Sie zu **UMS Administration > UMS Netzwerk > Server** und löschen Sie den Server mit der alten Prozess-ID.



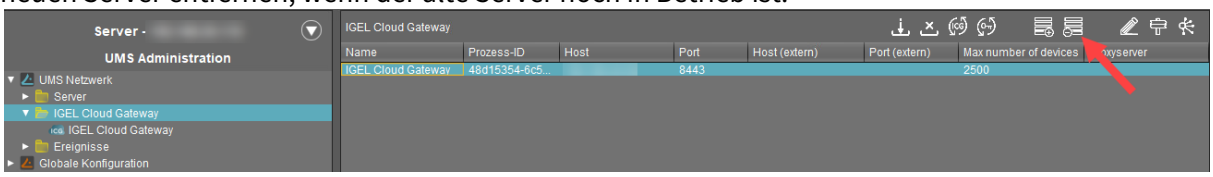
Nach den oben genannten Schritten können Sie den UMS Server jederzeit neu starten – die Verbindung zum ICG bleibt erhalten. Wenn Sie den UMS Server neu starten, bevor Sie die oberen Schritte durchgeführt haben, können Sie sich NICHT mit Ihrem bestehenden ICG verbinden und müssen es neu installieren.

ICG-Neuinstallation

Wenn Sie den UMS Server migriert oder neu installiert haben und aus irgendeinem Grund die oben beschriebene Methode nicht anwenden können, müssen Sie alle ICGs deinstallieren und neu installieren.

Nachdem Sie sich vergewissert haben, dass der neue / reinstallierte UMS Server ordnungsgemäß läuft, gehen Sie wie folgt vor:

1. Melden Sie sich am ICG-Host an und deinstallieren Sie das ICG, siehe ICG deinstallieren.
2. Starten Sie den ICG-Server neu.
3. Gehen Sie in der UMS Konsole zu **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway** und klicken Sie auf die Schaltfläche **Gateway aus der Datenbank entfernen**  , um das ICG vom UMS Server zu entfernen.
   Im Falle einer Migration des UMS Servers müssen Sie das ICG sowohl vom alten als auch vom neuen Server entfernen, wenn der alte Server noch in Betrieb ist.



4. Installieren Sie das ICG, und verbinden Sie es im Falle der Migration des UMS Servers nur mit dem neuen UMS Server. Siehe IGEL Cloud Gateway installieren.

- Für die Installation muss das gleiche Stammzertifikat verwendet werden.

- Das ICG darf nicht auf einen neuen Server umziehen und muss wie bisher erreichbar sein.

Tipp
Prüfen Sie vorab, ob ICG-Updates verfügbar sind, siehe IGEL Download Server[4]. Es wird außerdem empfohlen, Zeit und Datum auf allen UMS- und ICG-Servern sowie Ports (siehe IGEL UMS Kommunikationsports (see page 6)) zu überprüfen.

Nach der Neuinstallation des ICG können die zuvor gebundenen Endgeräte über das neue ICG verwaltet werden und müssen nicht neu registriert werden.

4 https://www.igel.com/software-downloads/enterprise-management-pack/

UMS verbindet sich nicht mit dem ICG: "TrustAnchor ...is not a CA certificate"

Symptom

Die UMS kann sich nicht mit dem IGEL Cloud Gateway (ICG) verbinden. Die folgende Nachricht erscheint auf der Bedienoberfläche oder in der Protokolldatei:

```
TrustAnchor ...is not a CA certificate
```

```
Caused by: sun.security.validator.ValidatorException: PKIX path validation
failed: sun.security.validator.ValidatorException: TrustAnchor with subject
"CN=UMS-CLUSTER--xxx, O=test, L=test, C=US" is not a CA certificate
at sun.security.validator.PKIXValidator.doValidate(PKIXValidator.java:380)
at sun.security.validator.PKIXValidator.engineValidate(PKIXValidator.java:273)
at sun.security.validator.Validator.validate(Validator.java:262)
at
sun.security.ssl.X509TrustManagerImpl.validate(X509TrustManagerImpl.java:327)
at
sun.security.ssl.X509TrustManagerImpl.checkTrusted(X509TrustManagerImpl.java:236
)
at
sun.security.ssl.X509TrustManagerImpl.checkServerTrusted(X509TrustManagerImpl.ja
va:113)
at
de.igel.apps.usg.connection.ssl.TrustedOnlyTrustManager.checkServerTrusted(Trust
edOnlyTrustManager.java:74)
at
sun.security.ssl.AbstractTrustManagerWrapper.checkServerTrusted(SSLContextImpl.j
ava:1099)
at
sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1622)
... 54 more
```

Umgebung

- UMS 6.04 oder höher
- ICG mit älteren Stammzertifikaten, die von UMS 5.07 oder UMS 5.08 erstellt wurden

Problem

Ältere ICG-Stammzertifikate (mit UMS 5.07 oder 5.08 erstellt) haben nicht den richtigen CA-Modifikator, was mit bisherigen Java-Versionen kein Problem darstellte. Die ab UMS 6.4.x verwendete Java-Version jedoch blockiert diese Zertifikate.

So prüfen Sie, ob Sie ein altes ICG-Stammzertifikat haben:

1. Öffnen Sie die UMS Konsole, gehen Sie zu **UMS Administration > Globale Konfiguration > Cloud Gateway Konfiguration** und selektieren Sie Ihr ICG-Stammzertifikat.
2. Klicken Sie  , um den Inhalt des Zertifikats anzusehen.
   Wenn **Certificate Authority** auf "false" gesetzt ist, haben Sie ein altes ICG-Stammzertifikat.

Lösung

Wenn Sie das ICG-Stammzertifikat nicht austauschen wollen (was eine Neuinstallation des ICG und eine erneute Registrierung aller Geräte bedeutet), können Sie einen Startparameter hinzufügen, der den UMS Server anweist, das CA-Flag im Zertifikat zu ignorieren.

> ⚠ Dieser Startparameter wird bei jedem Update der UMS überschrieben, so dass Sie ihn nach dem Update erneut setzen müssen.

Folgen Sie den Anweisungen unten, je nach verwendetem Betriebssystem.

Für Windows

1. Öffnen Sie den Windows-Dialog **Dienste** und stoppen Sie den Dienst **IGELRMGUIServer**.
2. Gehen Sie in das folgende Verzeichnis: `<UMS Installationsverzeichnis>\RemoteManager\rmguiserver\bin` (Beispiel: `C:\Program Files (x86)\IGEL\RemoteManager\rmguiserver\bin`)
3. Doppelklicken Sie **editTomcatService**.
4. Bestätigen Sie den Warndialog.
5. Wählen Sie die Registerkarte **Java**.
6. Fügen Sie unter **Java Options** den folgenden Eintrag als neue Zeile hinzu:
   `-Djdk.security.allowNonCaAnchor=true`
7. Klicken Sie **Ok**, um die Änderungen zu speichern.

Für Linux

1. Stoppen Sie den Dienst `igelRMserver`
2. Gehen Sie in das Verzeichnis `/opt/IGEL/RemoteManager/rmguiserver/bin`
3. Öffnen Sie die Datei `igelRMserver`

4. Fügen Sie vor jedem der beiden Einträge `-Xmx4096` eine neue Zeile mit folgendem Inhalt ein: `-Djdk.security.allowNonCaAnchor=true`
5. Speichern Sie die Änderungen.
6. Starten Sie den Dienst `igelRMserver`

Using Your Own Certificates for Communication over the Web Port (Default: 8443)

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

Wake on LAN

Bereitstellen eines Wake-on-LAN-Proxy für verteilte Umgebungen

Problem

Die UMS befindet sich außerhalb des Netzwerks, das Ihre Geräte enthält, so dass es Ihre Geräte nicht per Wake-on-LAN aufwecken kann.

Ziel

Sie möchten, dass die UMS Ihre Geräte von außerhalb ihres Netzwerks aufweckt.

Lösung

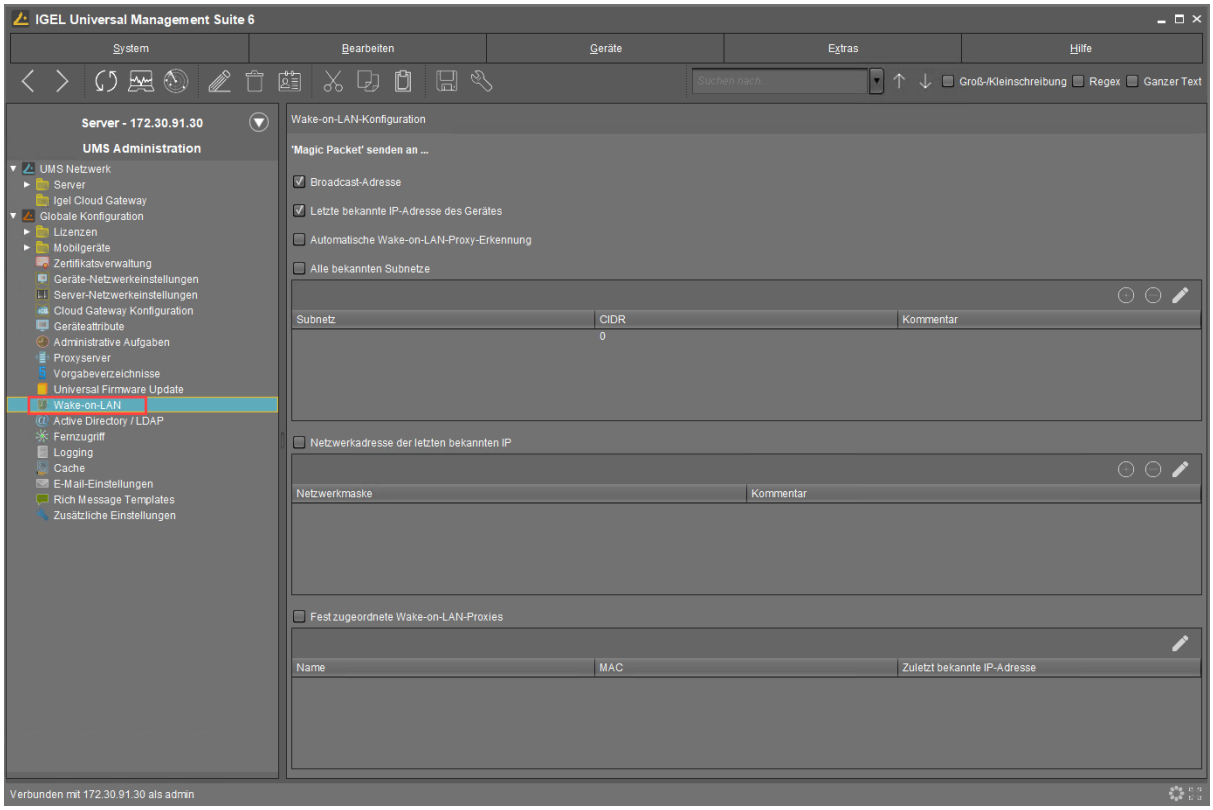
Wenn Sie die UMS Version 5.02.100 oder höher und Geräte mit Linux Version 5.09.100 oder höher verwenden, können Sie einen Geräte als Proxy verwenden, der die Wake-on-LAN-Pakete im Namen der UMS sendet.

Geräte als Wake-on-LAN-Proxy definieren

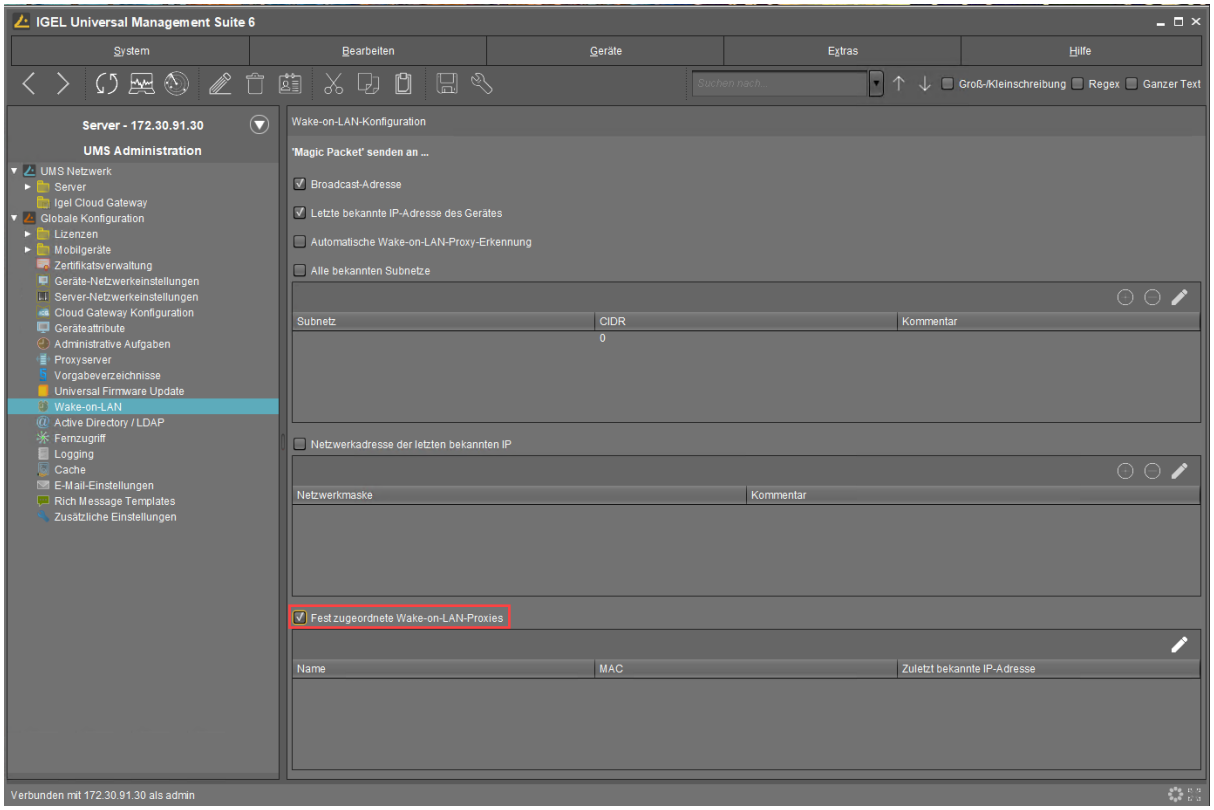
Sie können einen oder mehrere Geräte als Wake-on-LAN-Proxy definieren.

So definieren Sie ein Gerät als Wake-on-LAN-Proxy:

1. Melden Sie sich in der UMS Konsole an.
2. Gehen Sie in die **UMS Administration.**
3. Wählen Sie **Wake-on-LAN.**

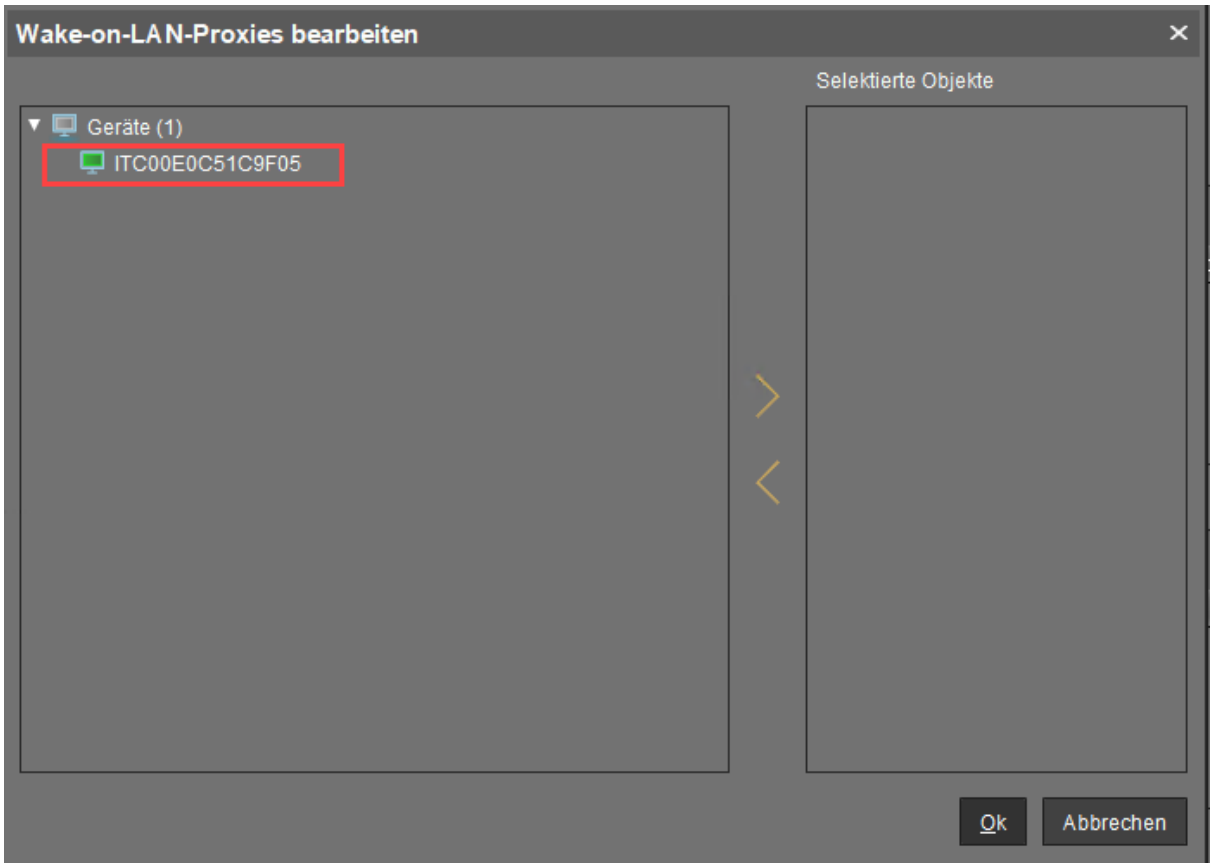


4. Aktivieren Sie **Fest zugeordnete Wake-on-LAN-Proxies.**

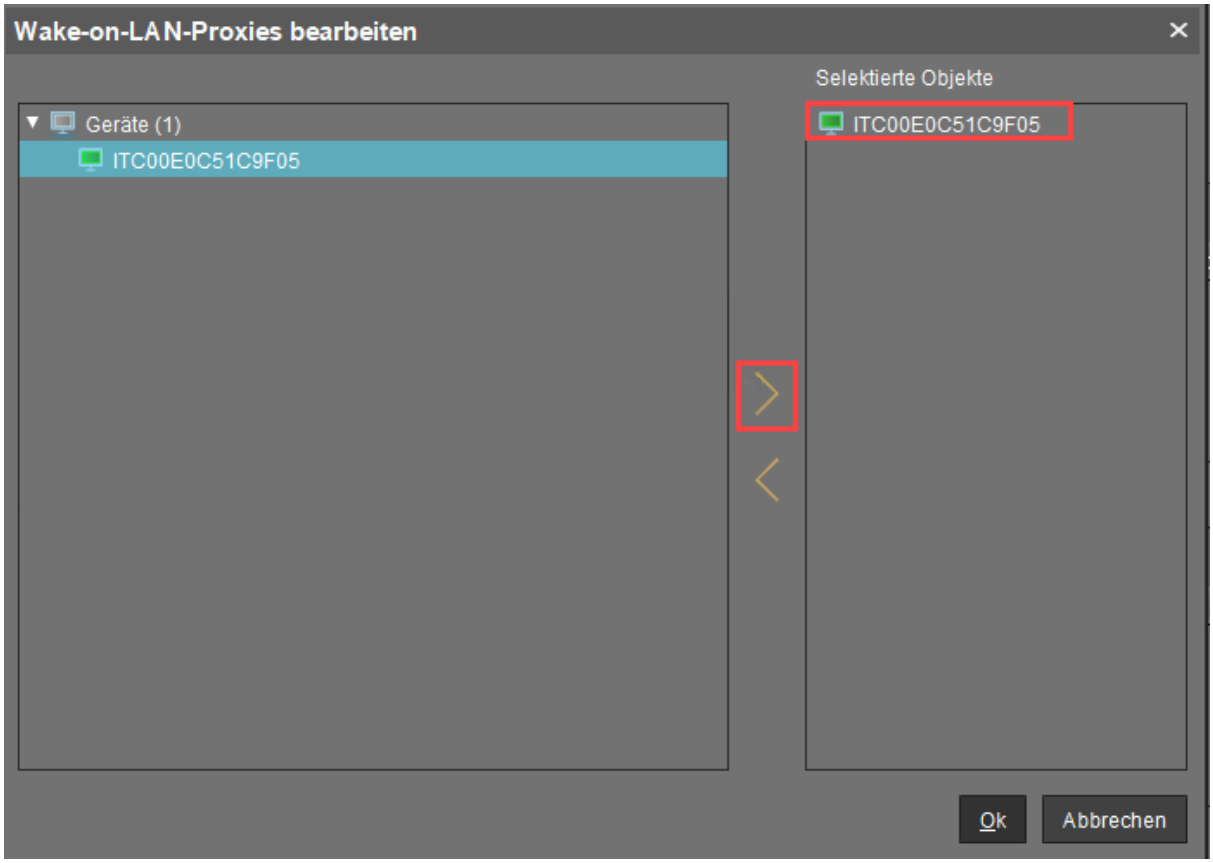


5. Klicken Sie auf  .
Der Dialog **Wake-on-LAN-Proxies bearbeiten** öffnet sich.

6. Wählen Sie das Gerät aus, das Sie als Wake-on-LAN-Proxy verwenden möchten.



7. Klicken Sie auf .
   Das ausgewählte Gerät wird unter **Selektierte Objekte** aufgelistet.



8. Klicken Sie **Ok.**
   Das ausgewählte Gerät ist als Wake-on-LAN-Proxy konfiguriert. In der Registry des Geräts wird der **Parameter** `system.remotemanager.wol_proxy.enabled` auf true gesetzt.

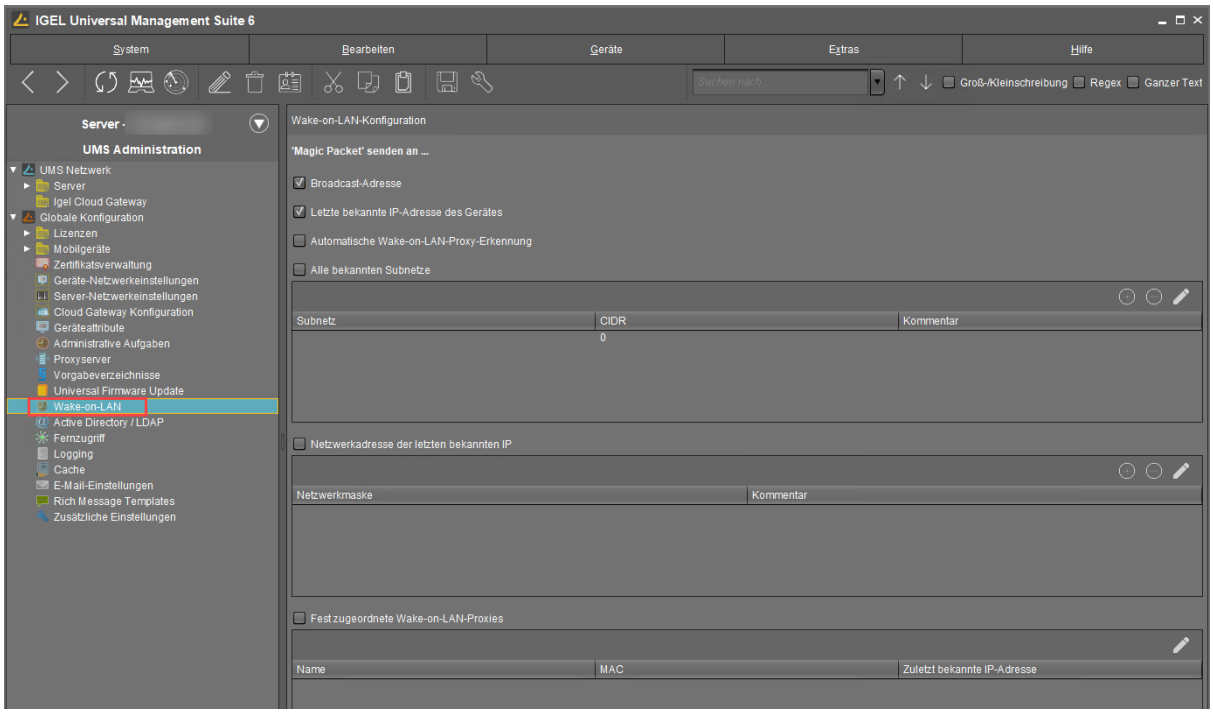
> Ein Gerät, das als Wake-on-LAN-Proxy konfiguriert ist, kann nicht auf Standby oder Herunterfahren eingestellt werden. Diese Sperre ist wirksam, sobald das Gerät seine Einstellungen von der UMS erhalten hat.

Einen Wake-on-LAN-Proxy entfernen

Sie können die Wake-on-LAN-Proxy Funktion von einem Gerät entfernen.

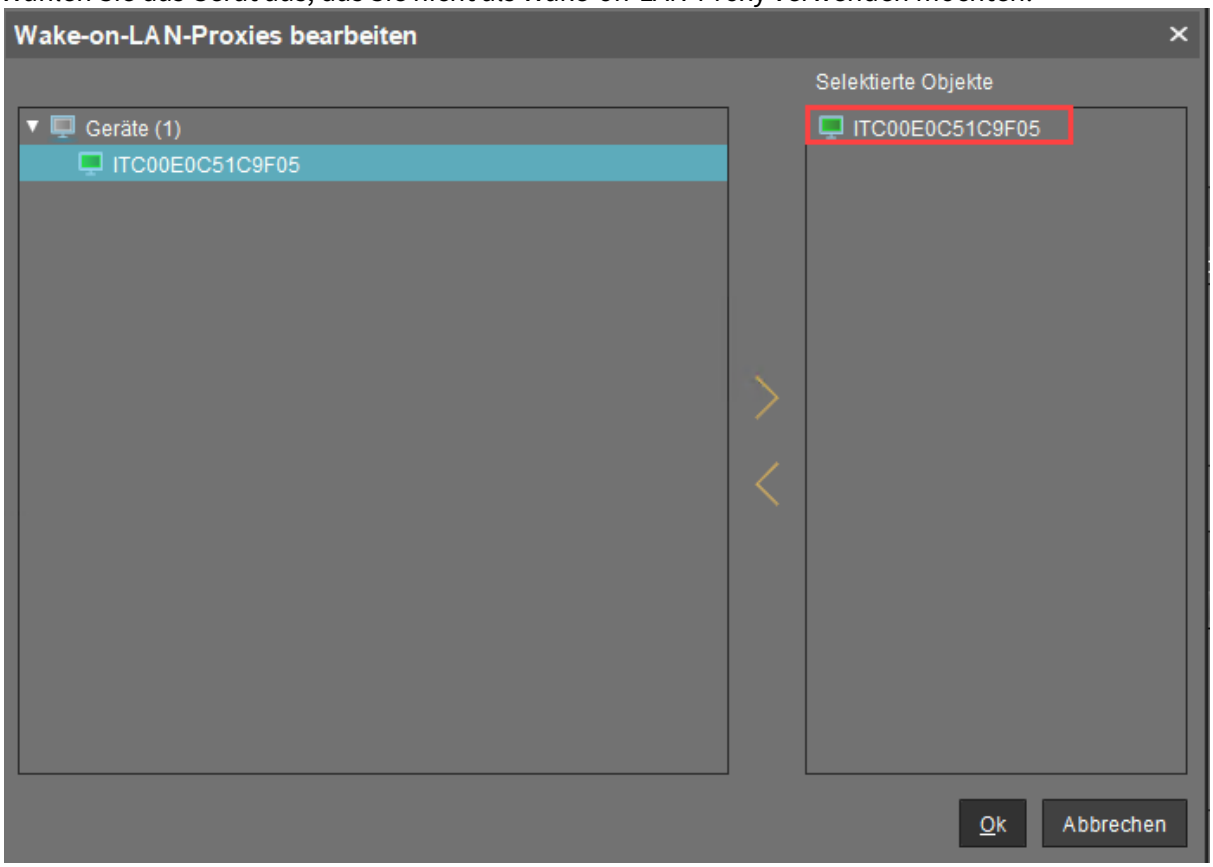
So definieren Sie einen oder mehrere Geräte als Wake-on-LAN Proxy:

1. Melden Sie sich in der UMS Konsole an.
2. Gehen Sie zu **UMS Administration**.
3. Wählen Sie **Wake-on-LAN.**



4. Klicke Sie auf  .
   Der Dialog **Wake-on-LAN-Proxies bearbeiten** öffnet sich.

5. Wählen Sie das Gerät aus, das Sie nicht als Wake-on-LAN-Proxy verwenden möchten.



6. Klicken Sie .
7. Klicken Sie **Ok**.
   Die ausgewählten Geräte ist nicht mehr als Wake-on-LAN-Proxy konfiguriert. Sobald das Gerät seine Einstellungen von der UMS erhalten hat, kann es in den Standbymodus versetzt und wie gewohnt heruntergefahren werden. In der Registry des Geräts wird der Parameter **system > remotemanager > wol_proxy > enabled** deaktiviert.

Verteilung von Wake on LAN-Paketen

Die IGEL UMS sendet die Magic Packets als UDP-Datagramme an Port 9. Damit esdas für verschiedene Subnetze funktioniert, muss dies von den beteiligten Routern unterstützt werden.

Wake-on-LAN-Einstellungen können in der **UMS Konsole** unter **UMS Administration > Globale Konfiguration > Wake-on-Lan-Konfiguration** konfiguriert werden.

Die UMS unterstützt das Senden von Wake-on-LAN Magic Packets an

- die Broadcast-Adresse
- die letzte bekannte IP Adresse des Geräts
- alle definierten Subnetze
- die Netzwerkadresse der letzten bekannten Thin Client-IP-Adresse (definieren Sie eine oder mehrere Netzwerkmasken, die angewendet werden sollen).
- einen dedizierten Wake on LAN Proxy, um Geräte in einem anderen Netzwerk aufzuwecken; siehe WoL-Proxy zum Aufwachen von Geräten verwenden (see page 135).

Über einen WoL-Proxy Thin Clients aufwecken

Sie haben die Möglichkeit, Geräte aufzuwecken, auch wenn sie in einem anderen Netzwerk verfügbar sind, das keine Broadcast-Pakete aus dem WAN zulässt. Ein Gerät, das als Wake-on-LAN-Proxy fungiert, versetzt sich nie selbst in den Standby-Modus, da es einen speziellen Weckruf aus der UMS abhören muss. Dieser Weckruf weist den Wake-on-LAN-Proxy an, Magic Packets an alle Geräte oder eine Auswahl von Geräten in seinem Netzwerk zu senden. Um diese Funktionalität zu unterstützen, muss der Wake-on-LAN-Proxy Geräte IGEL Linux Version 5.09.100 oder höher haben.

Sie können einen dedizierten Wake-on-LAN-Proxy definieren oder alternativ die UMS so einstellen, dass sie automatisch einen Wake-on-LAN-Proxy bestimmt. Letztere Option kann jedoch nicht garantieren, dass ein Wake-on-LAN-Proxy definiert werden kann, da dies davon abhängt, dass ein geeignetes Gerät im jeweiligen Subnetz online ist.

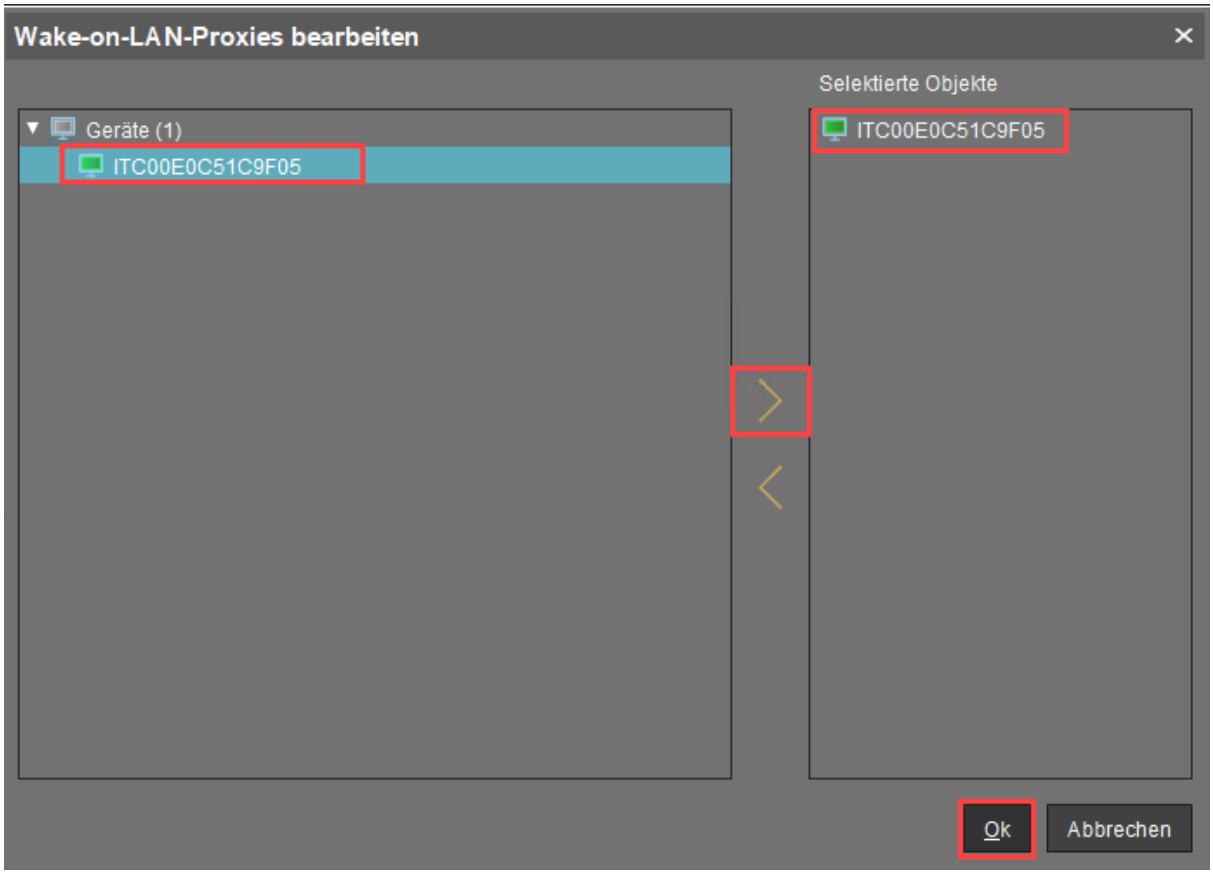
Detaillierte Informationen finden Sie im Kapitel Wake-on-LAN (see page 654) im Handbuch.

Um einen Wake-on-Lan-Proxy zu konfigurieren:

1. Gehen Sie auf **UMS Administration > Globale Konfiguration > Wake-on-Lan.**
2. Wählen Sie unter **'Magic Packet' senden an..."** die Adresse(n), an die der Weckruf gesendet werden soll (sollen).
3. Aktivieren Sie **Fest zugeordnete Wake-on-Lan-Proxies.**

4. Klicken Sie im unteren Bereich von **Wake-On-LAN-Proxies** auf die Schaltfläche .
5. Markieren Sie in der linken Spalte das gewünschten Gerät.
6. Klicken Sie auf um das Gerät zu wählen.

7. Klicken Sie **Ok**.



Das Gerät fungiert nun als ein Wake-on-LAN-Proxy.

> Ein Gerät, das als Wake-on-LAN-Proxy konfiguriert ist, kann nicht mehr in den Standby-Modus versetzt oder heruntergefahren werden. Diese Einschränkung gilt, sobald das Gerät die Einstellungen von der UMS erhält.

> Alternativ oder parallel kann man auch die **automatische WoL-Proxyerkennung** verwenden. Sie können jedoch nicht sicher sein, ob dieser Proxy immer läuft, während der **Fest zugeordnete WoL-Proxy** immer läuft.

Verwendung eines HTTP-Proxy für Firmware-Updates in UMS

Symptom

Sie möchten, dass die UMS Firmware-Updates aus dem Internet herunterlädt.

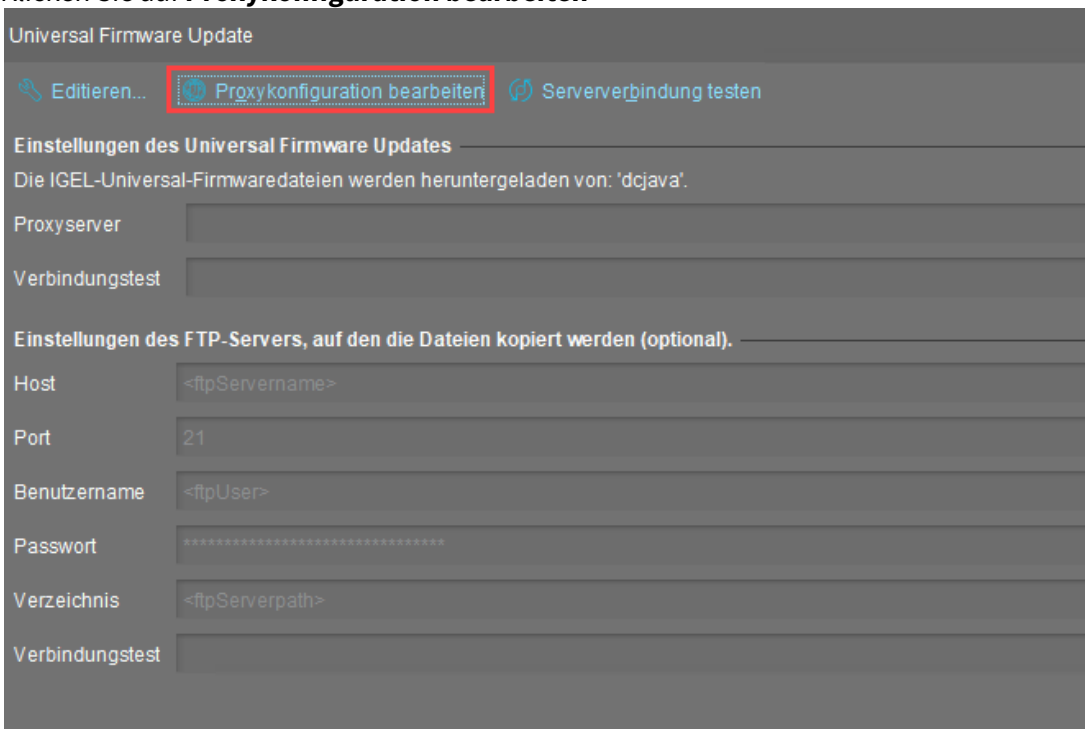
Problem

Der Internetzugang ist nur über einen HTTP-Proxy in Ihrer Umgebung möglich.

Lösung

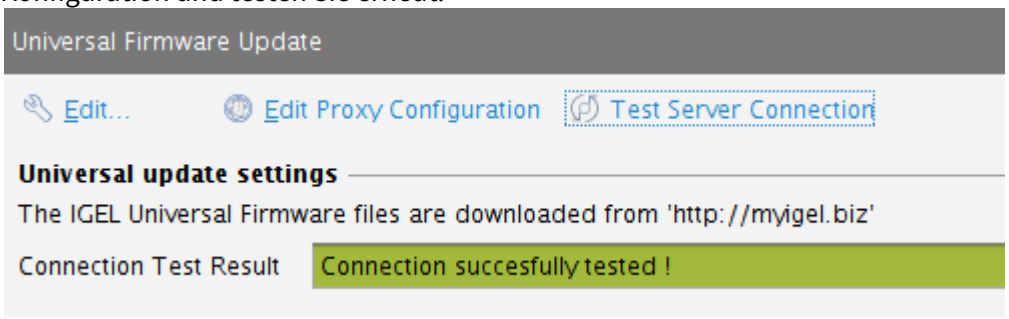
Konfigurieren Sie einen HTTP-Proxy für Firmware-Downloads in der UMS:

1. Gehen Sie in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Universal Firmware Update**
2. Klicken Sie auf **Proxykonfiguration bearbeiten**



3. Der **Proxykonfiguration bearbeiten** Dialog öffnet sich.
4. Aktivieren Sie **Verwenden Sie den Proxy für die HTTP-Verbindung zum Firmware-Update-Server.**
5. Geben Sie den Namen oder die IP Adresse des **Proxy-Host** ein.
6. Geben Sie den **Port** ein.
7. Geben Sie den **Benutzername** ein.
8. Geben Sie das **Passwort** ein.

9. Klicken Sie **Ok.**
   Der Dialog schließt sich.
10. Um die Verbindung über den Proxy zu testen, klicken Sie **Serververbindung testen.**
    Ein grüner Balken bedeutet Erfolg, wenn der Balken rot ist, überprüfen Sie Ihre Proxy-Konfiguration und testen Sie erneut.



UMS kann den Downloadserver nicht mehr kontaktieren

Symptom

Nachdem die UMS auf Version 6.03.130 oder höher aktualisiert wurde, kann sie den Downloadserver nicht mehr erreichen.

Umgebung

- UMS 6.03.130 oder höher

Problem

Ab UMS 6.03.130 kontaktiert die UMS https://fwus.igel.com (Port 443) anstatt http://fwu.igel.com (Port 80). Dies kann durch eine Firewall blockiert werden.

Lösung

▶ Lassen Sie https://fwus.igel.com (Port 443) in Ihrer Firewall zu.

Error During Firmware Upload in UMS: No Space on WebDAV

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Wie konfiguriere ich die Java-Heap-Größe für den UMS Server?

Sie haben Leistungsprobleme mit der IGEL Universal Management Suite (UMS). Die Gründe für die Leistungsverschlechterung können vielfältig sein, und es gibt verschiedene Lösungen wie z. B. die Optimierung der UMS gemäß den Empfehlungen unter Leistungsoptimierungen (see page 294), die Erweiterung des physischen Arbeitsspeichers des Servers, der Umstieg von der eingebetteten Datenbank zur externen Datenbank, die Aktualisierung der UMS Komponenten usw. Der folgende Artikel befasst sich aber ausschließlich mit der Vergrößerung des Speichers für den UMS Server (Java-Heap-Größe).

Symptom

Sie haben Leistungsprobleme, und die Protokolldateien des UMS Servers (`catalina.log` ; siehe Wo kann ich die IGEL UMS Logdateien finden? (see page 206)) deuten auf Speicherprobleme hin, z. B. `java.lang.OutOfMemoryError` .

Problem

Die standardmäßige Java-Heap-Größe kann für den UMS Server unzureichend sein. Dies kann in folgenden Fällen geschehen:

- große Anzahl von Jobs
- große Anzahl von administrativen Aufgaben
- große Anzahl von gleichzeitigen Geräteanfragen (z. B. Hunderte von Geräten, die in einem engen Zeitrahmen hochgefahren werden)
- eine große Anzahl von Geräten in der Datenbank (>10.000)
- die UMS Web App ist installiert
- eine Kombination der oben genannten Faktoren

Je mehr Jobs, administrative Aufgaben usw. erstellt werden, desto mehr Heap wird verbraucht, weswegen für zusätzliche Aufgaben nicht mehr genug Speicher vorhanden sein kann. In solchen Situationen kann es sinnvoll sein, die Java-Heap-Größe für den UMS Server zu erhöhen.

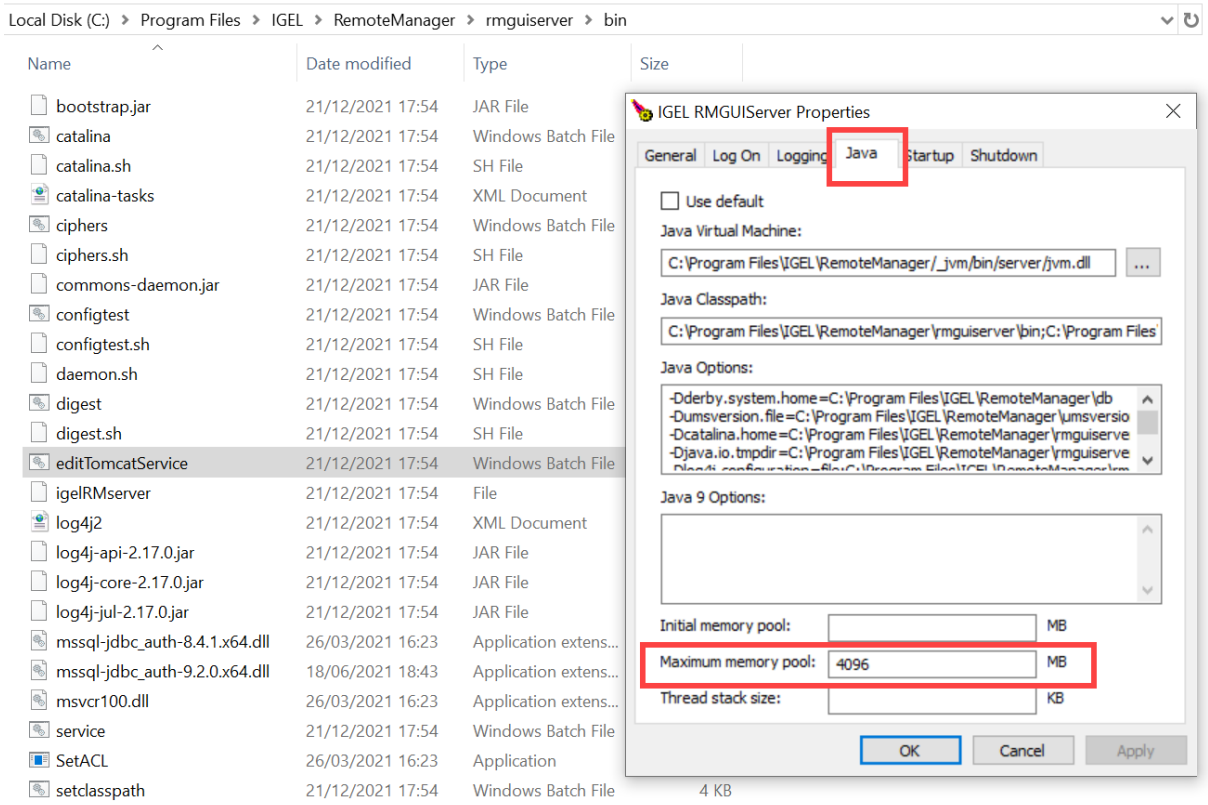
Lösung: Java-Heap-Größe für den UMS Server ändern

Windows

Für den unter Windows installierten UMS Server können Sie die Java-Heap-Größe während der UMS-Aktualisierung/Installation ändern. Einzelheiten hierzu finden Sie unter IGEL UMS unter Windows installieren (see page 266). Sie können die Java-Heap-Größe auch wie folgt anpassen:

1. Stoppen Sie den `IGEL RMGUIServer` -Dienst. Details dazu, wie Sie ihn stoppen können, finden Sie unter IGEL UMS HA-Dienste und -Prozesse (see page 949).

2. Navigieren Sie zu `C:\Program Files\IGEL\RemoteManager\rmguiserver\bin`.
3. Führen Sie `editTomcatService.bat` aus.
4. Wählen Sie die Registerkarte **Java** aus und passen Sie den Wert **Maximum memory pool** an Ihre Bedürfnisse an. (Standard: 4096 MB)



> ⚠ Die Java-Heap-Größe muss immer INDIVIDUELL, je nach Konfiguration des Servers und Ihrer UMS Umgebung, festgelegt werden, aber sie muss kleiner sein als der verfügbare physische RAM. Allgemeine Empfehlungen finden Sie im Oracle-Artikel Tuning Java Virtual Machines (JVMs)[5]; siehe dort auch die Option `-Xmx`.
>
> Beachten Sie auch das Folgende:
>
> - Alle Änderungen der Heap-Größe erfolgen auf eigenes Risiko! Ändern Sie die Heap-Größe nur, wenn Sie genau wissen, was Sie tun. Bei einer fehlerhaften Konfiguration kann es geschehen, dass der UMS Server nicht mehr läuft.
> - Eine Verringerung des Speichers kann die Funktion der UMS beeinträchtigen und wird NICHT empfohlen.

5 https://docs.oracle.com/cd/E15523_01/web.1111/e13814/jvm_tuning.htm#PERFM150

5. Klicken Sie **Ok**.
6. Starten Sie den `IGEL RMGUIServer`-Dienst neu.

Linux

So können Sie die Java-Heap-Größe für einen unter Linux installierten UMS Server anpassen:

1. Stoppen Sie den UMS Server-Prozess. Details dazu, wie Sie ihn stoppen können, finden Sie unter IGEL UMS HA-Dienste und -Prozesse (see page 949).
2. Bearbeiten Sie `/opt/IGEL/RemoteManager/rmguiserver/conf/ums-server.env`
3. Passen Sie in der Option `CATALINA_OPTS=-Xmx4096m` den Wert `-Xmx` entsprechend Ihren Anforderungen an. (Standard: 4096 MB)

   ⚠ Die Java-Heap-Größe muss immer INDIVIDUELL, je nach Konfiguration des Servers und Ihrer UMS Umgebung, festgelegt werden, aber sie muss kleiner sein als der verfügbare physische RAM. Allgemeine Empfehlungen finden Sie im Oracle-Artikel Tuning Java Virtual Machines (JVMs)[6]; siehe dort auch die Option `-Xmx`.

   Beachten Sie auch das Folgende:
   - Alle Änderungen der Heap-Größe erfolgen auf eigenes Risiko! Ändern Sie die Heap-Größe nur, wenn Sie genau wissen, was Sie tun. Bei einer fehlerhaften Konfiguration kann es geschehen, dass der UMS Server nicht mehr läuft.
   - Eine Verringerung des Speichers kann die Funktion der UMS beeinträchtigen und wird NICHT empfohlen.
   - Bei einer Aktualisierung der UMS wird der Wert für die Heap-Größe auf den Standardwert gesetzt. Daher müssen Sie ihn erneut anpassen.

4. Starten Sie den UMS Server-Prozess neu.

Ähnliche Themen

Wie konfiguriere ich die Java-Heap-Größe für die UMS Konsole? (see page 144)

Wie konfiguriere ich die Java-Heap-Größe für ICG?

6 https://docs.oracle.com/cd/E15523_01/web.1111/e13814/jvm_tuning.htm#PERFM150

Wie konfiguriere ich die Java-Heap-Größe für die UMS Konsole?

Sie verwenden die IGEL Universal Management Suite (UMS) und haben Leistungsprobleme mit der UMS Konsole. Die Gründe für die Leistungsverschlechterung können vielfältig sein, und es gibt verschiedene Lösungen wie z. B. die Optimierung der UMS gemäß den Empfehlungen unter Leistungsoptimierungen (see page 294), die Aktualisierung der UMS Komponenten usw. Der folgende Artikel befasst sich aber ausschließlich mit der Vergrößerung des Speichers für die UMS Konsole (Java-Heap-Größe).

Symptom

Sie haben Leistungsprobleme, und die Protokolldateien der UMS Konsole (`igel-ums-console.log` ; siehe Wo kann ich die IGEL UMS Logdateien finden? (see page 206)) deuten auf Speicherprobleme hin, z. B. `java.lang.OutOfMemoryError` .

Problem

Die standardmäßige Java-Heap-Größe kann für die UMS Konsole unzureichend sein. Dies geschieht normalerweise, wenn

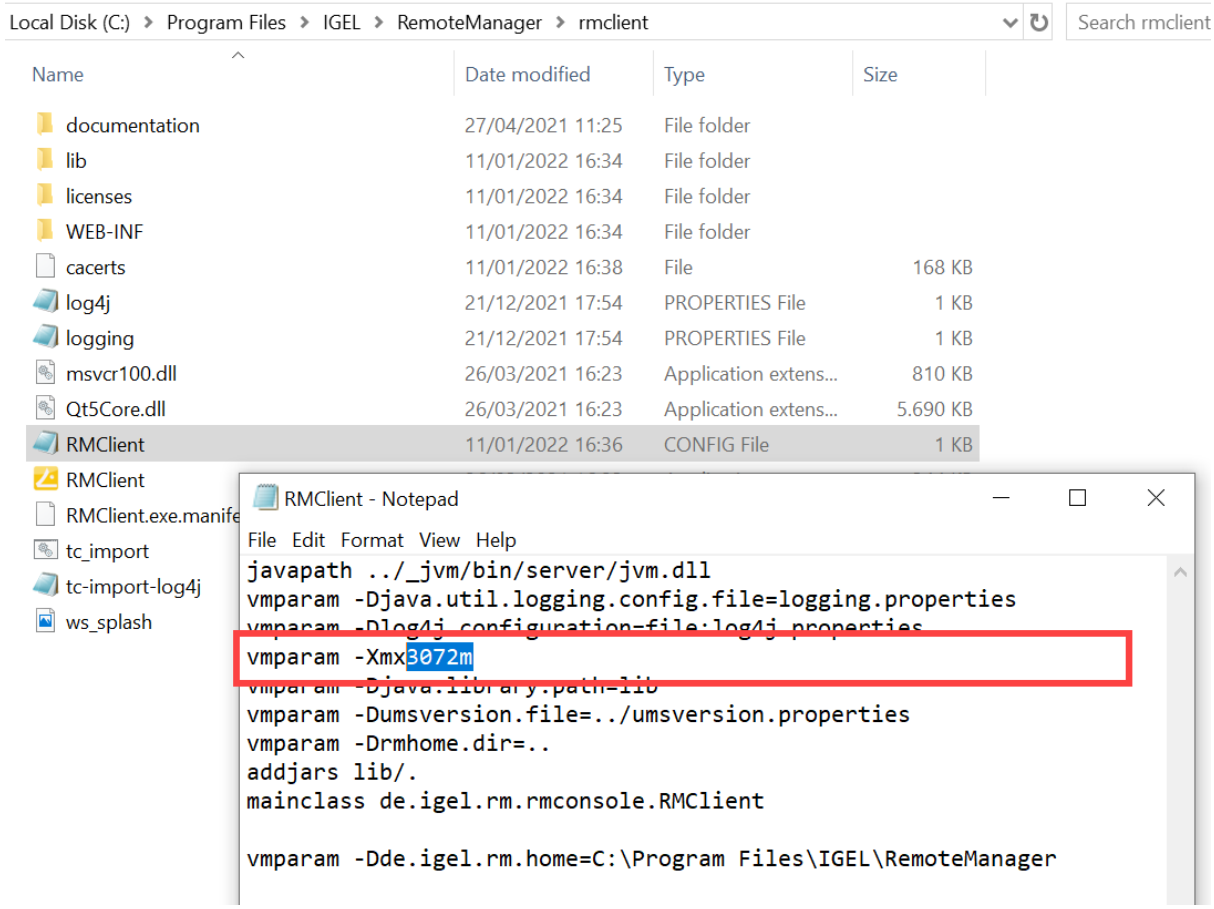
- eine große Anzahl von Geräten registriert ist (>10.000)
- viele Geräte in einen Ordner platziert wurden (eine flache Verzeichnisstruktur unter **Geräte** in der UMS Konsole; >1.000 pro Ordner)

Lösung: Java-Heap-Größe für die UMS Konsole ändern

Für die UMS Konsole können Sie die Java-Heap-Größe während der UMS-Aktualisierung/Installation ändern. Einzelheiten hierzu finden Sie unter IGEL UMS unter Windows installieren (see page 266). Sie können die Java-Heap-Größe auch wie folgt anpassen:

1. Schließen Sie die UMS Konsole.
2. Öffnen Sie die folgende Datei:
   Standardpfad unter Windows: `C:\Program Files\IGEL\RemoteManager\rmclient\RMClient.config`
   Standardpfad unter Linux: `/opt/IGEL/RemoteManager/rmclient/RemoteManager.config`

3. Passen Sie in der Zeile `vmparam -Xmx3072m` den Wert `-Xmx` entsprechend Ihren Anforderungen an. (Standard: 3072 MB)



⚠ Die Java-Heap-Größe muss immer INDIVIDUELL, je nach Konfiguration des Servers und Ihrer UMS Umgebung, festgelegt werden, aber sie muss kleiner sein als der verfügbare physische RAM. Allgemeine Empfehlungen finden Sie im Oracle-Artikel Tuning Java Virtual Machines (JVMs)[7]; siehe dort auch die Option `-Xmx` .

Beachten Sie auch das Folgende:

- Alle Änderungen der Heap-Größe erfolgen auf eigenes Risiko! Ändern Sie die Heap-Größe nur, wenn Sie genau wissen, was Sie tun. Bei einer fehlerhaften Konfiguration kann es geschehen, dass die UMS Konsole nicht mehr läuft.
- Eine Verringerung des Speichers kann die Funktion der UMS beeinträchtigen und wird NICHT empfohlen.

4. Speichern Sie die Änderungen.

7 https://docs.oracle.com/cd/E15523_01/web.1111/e13814/jvm_tuning.htm#PERFM150

5. Starten Sie die UMS Konsole neu.

Ähnliche Themen

Wie konfiguriere ich die Java-Heap-Größe für den UMS Server? (see page 141)

Wie konfiguriere ich die Java-Heap-Größe für ICG?

Wie überprüfe ich den aktuellen Status des IGEL UMS Servers über die vorhandene Monitoring Lösung?

IGEL Universal Management Suite (UMS) beinhaltet eine Monitoring-Endpoint-Lösung, die Sie in Ihre bestehende Monitoring-Infrastruktur (z.B. Nagios, SolarWinds, Paessler, Logic Monitor, Sensu, usw.) integrieren können. Mit dem Monitoring Endpoint können Sie die Prozess-/Servicezustände des UMS Servers überwachen und entsprechend reagieren, falls Probleme diagnostiziert werden.

IGEL Umgebung

- IGEL UMS 6.09.100 oder höher

Den aktuellen Status des UMS Servers abrufen

▶ Verwenden Sie die folgenden Anfragen, um den Status des UMS Servers zu überprüfen. Wenn Sie zu diesem Zweck einen Browser verwenden und die UMS ein selbstsigniertes Zertifikat hat, kann der Browser eine Sicherheits- / Zertifikatswarnung anzeigen. Akzeptieren Sie das Risiko und fahren Sie fort, oder machen Sie das Zertifikat dem Browser bekannt.

```
https://[server]:[web_server_port]/ums/check-status
```

ODER

```
http://[server]:[jws_server_port]/ums/check-status
```

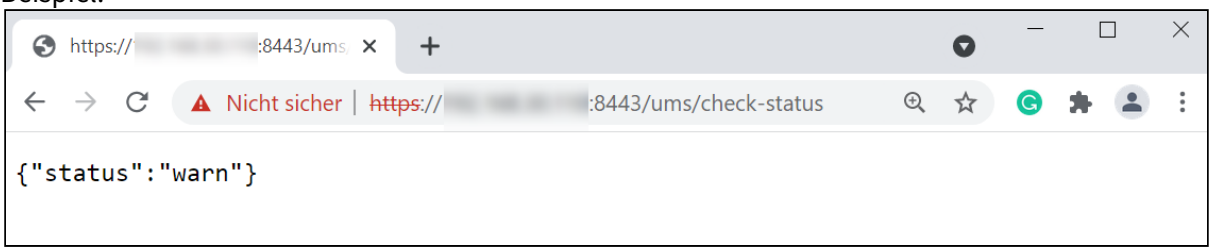
Die folgenden Antworten sind möglich:

1. Wenn der (Prüfstatus-) Dienst läuft, wird der HTTP-Statuscode 200 zurückgesendet. Der Antwortkörper enthält ein `JSON` -Dokument mit Informationen über den Status des UMS Servers:

   ```
   {“status”: ”init|ok|warn|err”}
   ```

   Details dazu finden Sie unter Den UMS Server überwachen: Mögliche Status (see page 148).

   Beispiel:

2. Wenn der Prüfstatusdienst nicht erreichbar ist, wird der HTTP-Statuscode 404 zurückgesendet.

3. Andere übliche HTTP-Statuscodes, die auf standardmäßige HTTP-Fehler hinweisen, können auftreten.

Beachten Sie, dass der Status des Servers jede Minute aktualisiert wird. Aus Leistungsgründen wird der Status NICHT bei jeder Überwachungsanforderung neu berechnet, d. h. wenn eine Überwachungsanforderung eingeht, aber ein 1-Minuten-Intervall noch nicht zu Ende ist, wird der zuvor gespeicherte Serverstatus angezeigt.

Den UMS Server überwachen: Mögliche Status

Die Antwortstatus, die während der Überwachung des UMS Servers zurückgesendet werden, deuten auf die folgenden Situationen hin:

ok	Der Server ist betriebsbereit und läuft.
warn	• Der Server ist im HA (see page 909)-Update-Modus, siehe Installation eines HA-Netzwerks aktualisieren (see page 931). • Der Server ist nicht mit einem oder mehreren konfigurierten IGEL Cloud Gateways verbunden, siehe Die UMS mit dem ICG verbinden. • Die für die Kommunikation mit den Endgeräten verwendeten Zertifikate (see page 573), d. h. die Zertifikate der Datei `tc.keystore`, sind nicht mit der Datenbank synchronisiert. Dies kann z. B. der Fall sein, wenn Sie Änderungen an den Zertifikaten vornehmen und währenddessen die automatische Synchronisierung aufgrund von Netzwerkproblemen aufhört zu funktionieren oder wenn das IGEL Netzwerktoken sich zwischen den Komponenten unterscheidet, was möglich ist, wenn z. B. bei der Serverinstallation ein falsches Netzwerktoken gewählt wurde.
err	• Es besteht keine Datenbankverbindung – keine Datenbank ist konfiguriert oder die Datenbankverbindung ist fehlgeschlagen, Wo Sie die Datenbank konfigurieren können, erfahren Sie unter Wie kann ich eine Datenquelle im IGEL UMS Administrator einrichten? (see page 730). • Der Port für die Gerätekommunikation ist nicht bereit. Wo Sie den Port für die Gerätekommunikation konfigurieren können, erfahren Sie unter Einstellungen - Servereinstellungen im IGEL UMS Administrator ändern (see page 709). Details über die UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).
init	Die Serverinitialisierung ist noch nicht abgeschlossen. Hinweis: Wenn der Initialisierungsprozess nicht innerhalb von 120 Sekunden abgeschlossen ist, wechselt der Status automatisch zu **err**.

Ähnliche Themen

Wie überwache ich das IGEL Cloud Gateway?

Configuring a Device to Send a Heartbeat Signal to the UMS (see page 147)

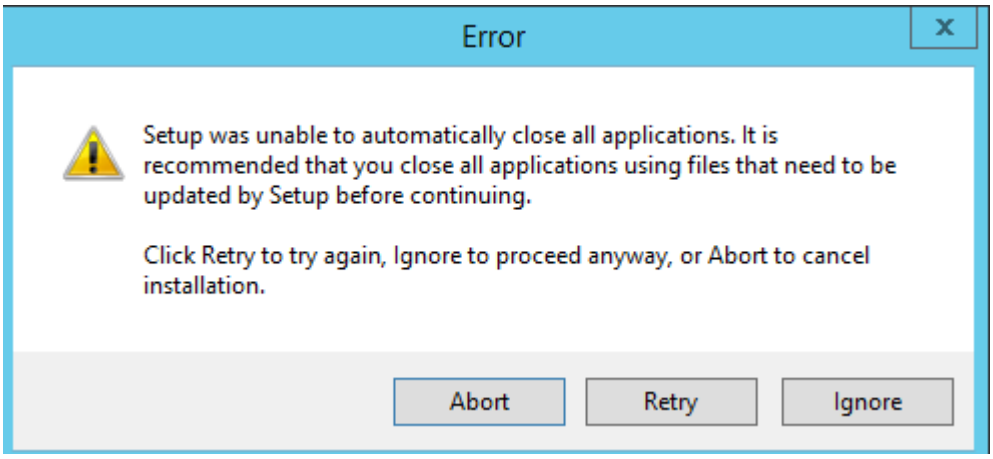
UMS HA Statusprüfung - Ihre High Availability- und Distributed UMS-Systeme analysieren (see page 944)

High Availability

Load Balancer stoppt nicht während der Aktualisierung der HA-Installation

Symptom

Bei der Aktualisierung der HA-Installation (High Availability) wird die Fehlermeldung angezeigt, dass nicht alle Anwendungen vor dem Update geschlossen werden konnten. Ein erneuter Versuch mit **Retry** löst das Problem nicht.

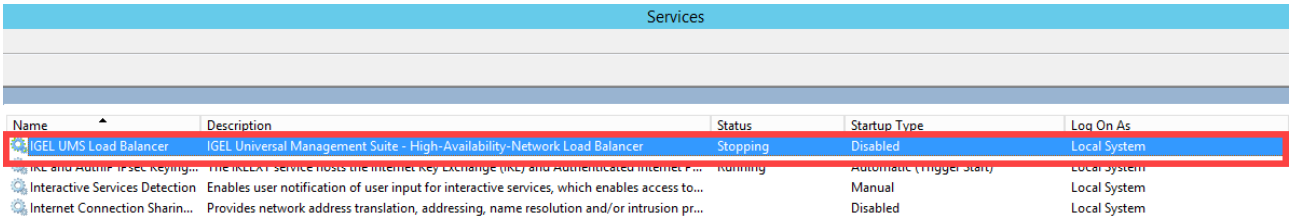


Umgebung

- HA-Installation

Problem

Der Load Balancer stoppt nicht und bleibt im "Stopping"-Modus:



Lösung

▶ Stoppen Sie den Load Balancer manuell und fahren Sie mit der Aktualisierung fort. Für Informationen zum Stoppen der HA-Dienste siehe IGEL UMS HA-Dienste und -Prozesse (see page 949).

Welche Dateien werden automatisch zwischen den IGEL UMS Servern synchronisiert?

Sie haben eine IGEL Universal Management Suite (UMS) Installation mit mehreren Instanzen (see page 246) und möchten wissen, welche Dateien automatisch zwischen den Servern synchronisiert werden.

Voraussetzungen

- Eine HA-Umgebung (High Availability) mit UMS Version 6.06.100 oder höher
- Eine Distributed UMS-Installation mit UMS Version 6.10.100 oder höher

Allgemeiner Überblick

Folgende Dateien werden zwischen den UMS Servern automatisch synchronisiert:

- Dateien, die in der UMS Konsole registriert sind

  > Dateien, die nicht als Dateiobjekte in der UMS angelegt, sondern nur im Dateisystem in `ums_filetransfer` gespeichert sind, werden NICHT synchronisiert. Einzelheiten dazu, wie/wo Sie ein Dateiobjekt erstellen können, finden Sie unter Dateien - Dateien am IGEL UMS Server registrieren und zu Geräten übertragen (see page 529) und Firmwareanpassung erstellen (see page 436).

- Universal Firmware Updates (see page 539), falls die Synchronisierung unter **UMS Administration > Globale Konfiguration > Universal Firmware Update** aktiviert ist und ein WebDAV-Verzeichnis als Zielpfad für das Herunterladen festgelegt ist. Einzelheiten finden Sie unten im Abschnitt "Synchronisierung der Universal Firmware Updates (see page 151)".

Die Objekte werden sofort synchronisiert, sofern ein UMS Server vorübergehend unerreichbar ist. In diesem Fall findet die Synchronisierung alle 5 Minuten oder beim Serverstart statt.

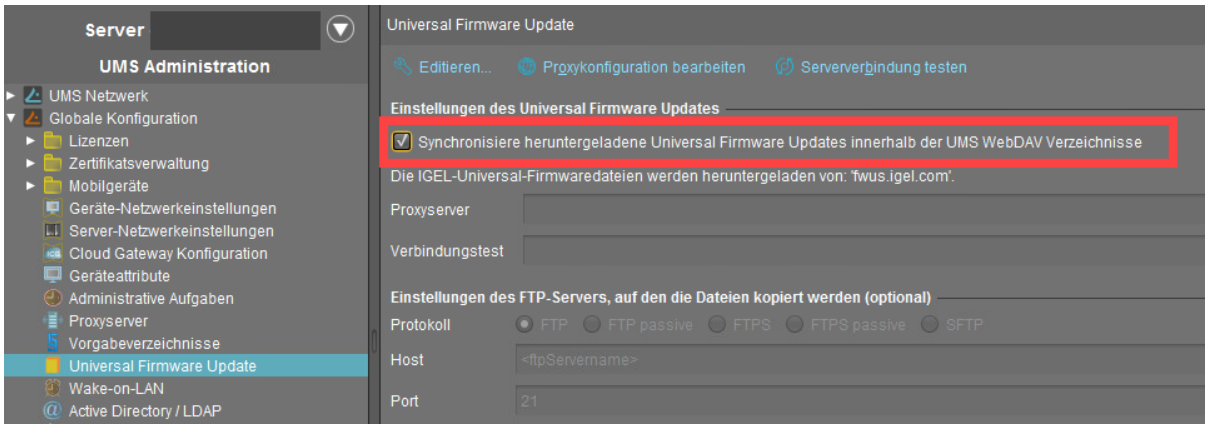
Die Synchronisierung bezieht sich auf das Dateisystem und aktualisiert die Ansicht in keiner anderen UMS Konsole als derjenigen, in der das Objekt erstellt wurde. Daher müssen Sie eventuell [F5] oder die Aktualisierungsschaltfläche  drücken, um das Objekt in der UMS Konsole auf dem anderen Server anzusehen.

> Um Probleme mit Ihrer HA-Installation zu vermeiden, stellen Sie sicher, dass der Zeitunterschied auf den Servern des HA-Netzwerks eine Minute nicht überschreitet. Nach jeder manuellen Zeitänderung müssen die HA-Dienste auf dem entsprechenden Server neu gestartet werden.

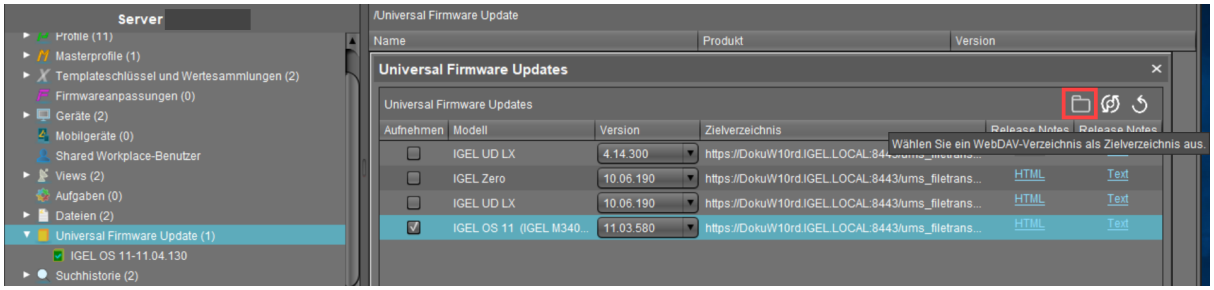
Synchronisierung der Universal Firmware Updates

So aktivieren Sie die automatische Synchronisierung der Firmwareupdates zwischen den UMS Servern:

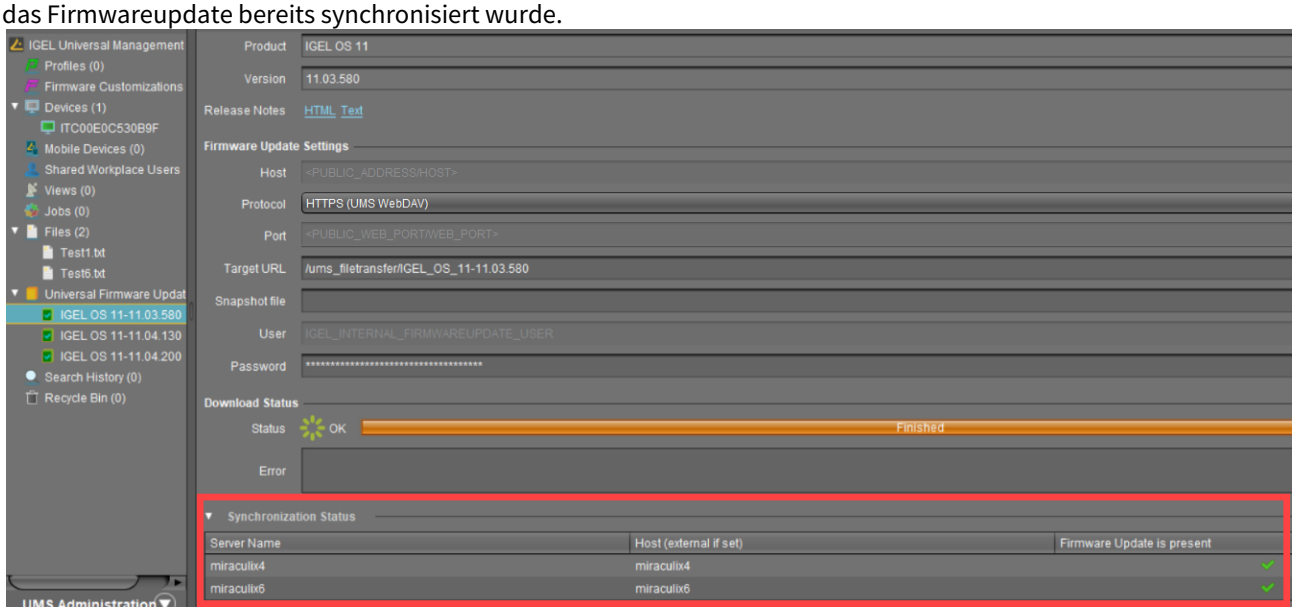
1. Gehen Sie in der UMS Konsole auf **UMS Administration > Globale Konfiguration > Universal Firmware Update**.
2. Aktivieren Sie **Synchronisiere heruntergeladene Universal Firmware Updates innerhalb der UMS WebDAV Verzeichnisse**.



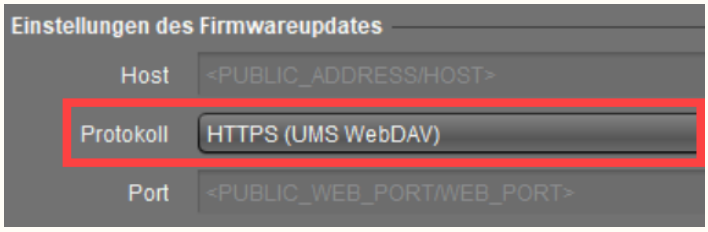
3. Wenn Sie ein Firmwareupdate unter **Universal Firmware Update > [Kontextmenü] > Neue Universal Firmware Updates suchen** hinzufügen, legen Sie ein WebDAV-Verzeichnis als Zielpfad für das Herunterladen fest.



Wenn das Herunterladen abgeschlossen ist, können Sie unter **Synchronisierungsstatus** die Server sehen, für die das Firmwareupdate bereits synchronisiert wurde.



⚠ Universal Firmware Updates werden zwischen den UMS Servern nur dann synchronisiert, wenn **HTTPS (UMS WebDAV)** oder **HTTP (UMS WebDAV)** unter **Protokoll** ausgewählt ist. Diese Protokolle werden für die Übertragung der Firmwareupdate-Dateien aus dem UMS WebDAV-Verzeichnis an die Geräte verwendet.



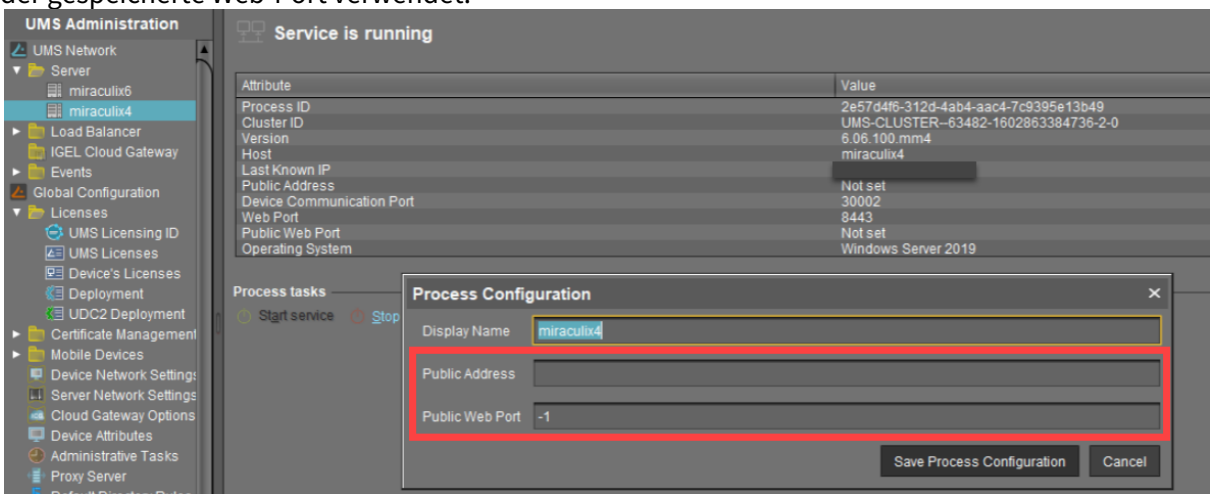
Mit den sonstigen Protokollen werden Firmwareupdates zwischen den UMS Servern nicht synchronisiert.

Während der Aktualisierung verwendete Verbindungsdaten

Wenn einem Gerät ein Firmwareupdate zugewiesen wird, werden die Verbindungsinformationen des aktuellen Servers an das Gerät gesendet, falls das Firmwareupdate im UMS WebDAV-Verzeichnis des Servers vorhanden ist. Wenn das Firmwareupdate aus irgendeinem Grund nicht vorhanden ist, werden die Verbindungsinformationen eines Servers mit dem verfügbaren Firmwareupdate gesendet.

Die Verbindungsinformationen enthalten

- eine **Öffentliche Adresse**, wenn sie für den Server unter **UMS Administration > UMS Netzwerk > Server > [Kontextmenü des Servers] > Editieren** konfiguriert ist. Andernfalls wird der gespeicherte Hostname verwendet.
- einen **Öffentlichen Web-Port**, wenn er für den Server unter **UMS Administration > UMS Netzwerk > Server > [Kontextmenü des Servers] > Editieren** konfiguriert ist. Andernfalls wird der gespeicherte Web-Port verwendet.



Da die Verbindungsinformationen dynamisch angepasst werden, sind Angaben für **Host** und **Port** für das heruntergeladene Firmwareupdate nicht editierbar (mit eingestelltem HTTP(S) (UMS WebDAV)-Protokoll):


Shared Workplace-Benutzer
Views (2)
Aufgaben (0)
Dateien (2)
Universal Firmware Update (2)
IGEL OS 11-11.03.580
IGEL OS 11-11.04.130
Einstellungen des Firmwareupdates
Host
<PUBLIC_ADDRESS/HOST>
Protokoll
HTTPS (UMS WebDAV)
Port
<PUBLIC_WEB_PORT/WEB_PORT>
Ziel-URL
/ums_filetransfer/IGEL_OS_11-11.03.580

Lastverteilung mit mehreren Load Balancern

Wenn ein UMS Server und Load Balancer auf einem gemeinsamen Computer installiert sind, kommuniziert der UMS Server mit den IGEL OS 11 Endgeräten über Port 30002, ansonsten über Port 30001, wie es bei einer einzelnen Serverinstallation üblich ist. Der Load Balancer kommuniziert immer mit den IGEL OS 11 Geräten über den Port 30001.

Die Lastverteilung auf die Load Balancer kann wie folgt durchgeführt werden. Beim Booten versuchen die OS 11 Geräte in dieser Reihenfolge, Kontakt mit dem UMS Server aufzunehmen:

- DHCP-Tag 224
- Name `igelrmserver` in der DNS (Eintragstyp A)
- Lokale Liste der **Remote Management Server** (in der angegebenen Reihenfolge)

In einem UMS High-Availability-Netzwerk werden die Load Balancer in der Liste der Remote Management Server in der lokalen Gerätekonfiguration automatisch angegeben.

Wird der DNS-Eintrag `igelrmserver` oder DHCP-Tag 224 in einem HA-Netzwerk verwendet, muss die IP eines Load Balancers eingegeben werden.

Wenn weder dieser DNS-Eintrag noch der DHCP-Tag 224 verwendet wird, verbinden sich Endgeräte immer mit dem ersten Load Balancer in der Setup-Liste, d. h. alle Geräte kommunizieren mit einem einzigen Load Balancer. Die anderen Load Balancer sind lediglich Stand-by und werden nur verwendet, wenn der erste Load Balancer in der Liste nicht verfügbar ist.

Um eine Lastverteilung zwischen den Load Balancern zu erreichen, können Sie jedoch den DNS-Eintrag `igelrmserver` mit einer Lastverteilung per DNS verwenden. Dazu werden die IP-Adressen aller Load Balancer im DNS als Resource Record Set für den `igelrmserver`-Eintrag erfasst (vgl. https://de.wikipedia.org/wiki/Lastverteilung_per_DNS). Die Geräte verbinden sich dann zufällig mit einem der verfügbaren Load Balancer und verteilen so die Abfragelast aller Geräte.

License Error Because HA Servers Are out of Sync

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Manuelle Synchronisierung der UMS-ID

Wenn die Haupt-UMS-ID zwischen den IGEL UMS Servern nicht synchronisiert ist, lautet der **Status der UMS-ID** unter **UMS Administration > Globale Konfiguration > UMS ID** "Nicht synchron, bitte Server neustarten", siehe UMS ID (see page 639). Aber selbst wenn Sie den UMS Server neu starten, bleibt die UMS-ID manchmal unsynchronisiert. In diesem Fall ist die manuelle Synchronisierung erforderlich.

Umgebung

- UMS 12.01.100 oder höher
- High-Availability (HA)- oder Distributed UMS-Umgebung

Anleitung

Die manuelle Synchronisierung der UMS-ID umfasst die folgenden Schritte:

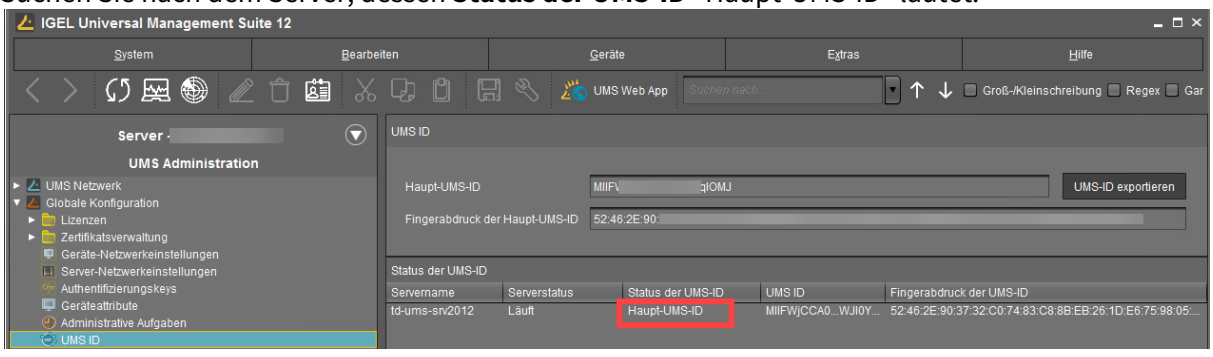
1. Feststellen, auf welchem Server sich die Haupt-UMS-ID befindet (see page 157)
2. Ein Backup der UMS-ID auf diesem Server erstellen (see page 157)
3. Das erstellte Backup auf allen Servern mit einer unsynchronisierten UMS-ID wiederherstellen (see page 158) und alle Server neu starten

Feststellen, auf welchem Server sich die Haupt-UMS-ID befindet

So finden Sie heraus, welcher Server der HA- oder Distributed UMS-Installation die **Haupt-UMS-ID** besitzt:

1. Öffnen Sie die UMS Konsole und navigieren Sie zu **UMS Administration > Globale Konfiguration > UMS ID**.

2. Suchen Sie nach dem Server, dessen **Status der UMS-ID** "Haupt-UMS-ID" lautet.



Ein Backup der UMS-ID erstellen

1. Gehen Sie auf den Server mit der Haupt-UMS-ID, den Sie im vorherigen Schritt lokalisiert haben, und öffnen Sie den UMS Administrator.

2. Gehen Sie auf **UMS-ID-Sicherung** und erzeugen Sie ein Backup wie unter UMS-ID-Sicherung im IGEL Administrator (see page 713) beschrieben.

3. Übertragen Sie das erstellte Backup auf jeden Server mit einer unsynchronisierten UMS-ID.

Das Backup auf allen Servern mit einer unsynchronisierten UMS-ID wiederherstellen

1. Öffnen Sie den **UMS Administrator** auf jedem Server, auf dem die UMS-ID nicht synchronisiert ist.
2. Gehen Sie auf **UMS-ID-Sicherung** und stellen Sie das Backup wieder her, wie unter UMS-ID-Sicherung im IGEL Administrator (see page 713) beschrieben.
3. Wiederholen Sie den Vorgang für alle Server mit einer unsynchronisierten UMS-ID.
4. Wenn das Wiederherstellungsverfahren abgeschlossen ist, starten Sie alle Server neu, falls Sie dies noch nicht getan haben.
   In der UMS Konsole sollte der **Status der UMS-ID** unter **UMS Administration > Globale Konfiguration > UMS ID** anzeigen, dass die UMS-ID nun auf allen Servern synchronisiert ist.

Error Message When Switching Back from an Externally Signed CA to the Internal CA

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

How to Migrate an UMS High Availability Installation to a Standalone UMS

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

How to Migrate HA UMS to a Distributed UMS

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Troubleshooting: UMS 12 HA Not Working After Upgrade

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Geräte

- Thin Client Scan oder Online Überprüfung schlägt fehl
- Die Registrierung eines Thin Clients schlägt fehl
- Thin Client Registrierung schlägt fehl mit Fehlermeldung "Unerwartetes Ende des Input-Streams"
- Die Geräteregistrierung hinter der SonicWall Firewall schlägt fehl.
- Den Hostnamen eines Geräts über die UMS ändern

Geräte Scan oder Online Überprüfung schlägt fehl

Symptom

Obwohl ein Gerät auf einen Ping-Befehl reagiert, erscheint er nicht in der Liste der gescannten Geräte der UMS Konsole, kann nicht registriert werden oder erscheint als offline (rot) im Navigationsbaum der UMS Konsole.

Problem

Die Pakete zum Scannen der Geräte oder zur Überprüfung ihres Online-Status werden im Netzwerk blockiert, z. B. durch eine Firewall oder ein VPN.

Lösung

Stellen Sie sicher, dass UDP Pakete auf Port 30005 nicht in Ihrem Netzwerk blockiert werden. Diese Pakete werden sowohl für das Scannen nach Geräten als auch für die Überprüfung des Status der Clients verwendet.

Sehen Sie auch IGEL UMS Communication Ports (see page 6).

Troubleshooting: Die Registrierung eines Geräts über Suche nach Geräten schlägt fehl

Der folgende Artikel erläutert die möglichen Ursachen und Lösungen für eine fehlgeschlagene Geräteregistrierung an der IGEL Universal Management Suite (UMS) wenn Sie die Scan- und Registrierungsmethode verwenden. Einzelheiten zu dieser Methode finden Sie unter Scanning the Network for Devices and Registering Devices on the IGEL UMS (see page 324).

Symptom

Obwohl ein Gerät von der Konsole aus gescannt werden kann, kann es nicht auf dem Server registriert werden. Eine der folgenden Fehlermeldungen erscheint in der UMS Konsole:

- `Cannot connect to remote management server`
- `Protocol state invalid`
- `Certificate invalid`

Problem

Dies kann folgende Ursachen haben:

- die Firewall des Servers blockiert den Prozess
- ein bereits existierendes UMS Zertifikat auf dem Gerät
- ein Datenbankdienst hängt
- Verzögerungen oder Verluste bei der Netzwerkübertragung, die den Registrierungsprozess beeinträchtigen
- nicht korrekte Zeit / Datum auf dem Gerät oder dem UMS Server

Lösung

Lösung des Firewall-Problems

1. Fügen Sie auf Ihrem System, auf dem die UMS Konsole und der UMS Server laufen, den folgenden Port als Ausnahme in der Windows-Firewall hinzu:
   - **Name** = `IGEL RMGUIServer`
   - **TCP Port** = `30001`

   > Wenn Sie den Standardport 30001 im UMS Administrator geändert haben, öffnen Sie die Firewall entsprechend für diesen Port. Mehr Informationen zu den Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).

2. Stellen Sie sicher, dass keine andere Firewall im Netzwerk die Ports 30001 und 30005 blockiert.
3. Versuchen Sie, das Gerät erneut zu importieren.

> Es kann auch hilfreich sein, die SSL-Inspektion in der Netzwerk-Firewall zu überprüfen.

Lösung des Zertifikatsproblems

Für OS 11 Geräte:

▶ Löschen Sie auf dem Gerät das Zertifikat `server.crt` aus dem Ordner `/wfs/`. Versuchen Sie, das Gerät erneut zu registrieren.

ODER

▶ Wenn Sie wissen, von welchem UMS Server genau das Gerät das Zertifikat erhalten hat und Zugriff auf diesen UMS Server haben, können Sie das Zertifikat so entfernen, wie unter UMS Zertifikat vom OS 11 Gerät entfernen (see page 220) beschrieben.

Für OS 11 oder OS 12 Geräte:

▶ Setzen Sie das Gerät auf die Werkseinstellungen zurück und versuchen Sie, das Gerät erneut zu registrieren. Wie Sie das IGEL OS-Gerät auf die Werkseinstellungen zurücksetzen können, erfahren Sie unter Reset to Factory Defaults.

Lösung des Datenbankproblems

▶ Deaktivieren Sie im **UMS Administrator > Datenquelle** die aktuell aktive Datenquelle und aktivieren Sie sie erneut. Versuchen Sie, das Gerät erneut zu registrieren.

Einzelheiten zum UMS Administrator finden Sie unter Der IGEL UMS Administrator (see page 707).

Netzwerk überprüfen

▶ Überprüfen Sie, ob das Netzwerk in Ordnung ist, indem Sie Pings von der Gerätekonsole an Ihren UMS Server senden:

```
ping -s -c 10 -M do
```

Beginnen Sie mit SIZE =1500 und verringern Sie die Größe der Pakete, bis alle Pakete ohne Fragmentierung oder Paketverlust übertragen wurden. 1440 / 1400 / 1350 / 1300 sind gute Werte zum Testen.

> Auf einem Gerät mit IGEL OS können Sie zum " Pingen" des UMS Servers die integrierten Netzwerktools verwenden (standardmäßig: **Startmenü > System > Netzwerkdiagnose**; siehe Netzwerkdiagnose).

Zeit und Datum überprüfen

▶ Überprüfen Sie, ob die Zeit und das Datum auf dem Gerät (siehe Zeit und Datum) und auf dem UMS Server korrekt eingestellt sind.

Tipp
Wenn Sie Probleme mit der Geräteregistrierung in der UMS haben, empfiehlt es sich generell zu prüfen

- ob die Registrierung direkt vom Endgerät aus funktioniert, siehe UMS Registration. Falls nicht, deutet dies in der Regel auf ein Netzwerkproblem hin.
- ob es eine andere UMS im Netzwerk gibt und die DHCP- und/oder DNS-Serverkonfiguration auf die "falsche" UMS verweist.

Ähnliche Themen

Geräte Registrierung schlägt fehl mit Fehlermeldung "Unerwartetes Ende des Input-Streams" (see page 168)

Die Geräteregistrierung hinter der SonicWall Firewall schlägt fehl. (see page 169)

Geräte Scan oder Online Überprüfung schlägt fehl (see page 164)

Geräte Registrierung schlägt fehl mit Fehlermeldung "Unerwartetes Ende des Input-Streams"

Symptom

Die UMS Konsole zeigt eine Fehlermeldung wie "Unerwartetes Ende des Input-Streams gefunden bei..." während der Registrierung von Geräten an.

Problem

Geräte können sich aufgrund von Problemen mit großen Paketen nicht über eine Remote-Verbindung über VPN-Gateway, Router, Firewall oder andere Netzwerkgeräte mit UMS anmelden.

Der Fehler kann auch dann auftreten, wenn kein NAT verwendet wird und das Netzwerkgerät korrekt konfiguriert zu sein scheint, so dass z. B. das Pinging in beide Richtungen erfolgreich ist.

Lösung

Bitte lesen Sie die Dokumentation zu Ihrem Netzwerkgerät und informieren Sie sich über die Möglichkeiten zur Handhabung großer Pakete. Bei SonicWall-Geräten setzt die Lösung die Option `Ignore Don't Fragment Bit`.

Die Geräteregistrierung hinter der SonicWall Firewall schlägt fehl.

Symptom

Die Geräte werden vom UMS während eines Scans erkannt, aber die Registrierung schlägt fehl. Die UMS Konsole zeigt eine Fehlermeldung wie "Unerwartetes Ende des Input-Streams gefunden bei....".

Mögliche Ursachen

Die folgenden Ursachen wurden von SonicWall mit Firewalls gemeldet;

- Große Pakete: Sehen Sie Geräte Registrierung schlägt fehl mit Fehlermeldung "Unerwartetes Ende des Input-Streams" (see page 168).
- SonicWall DPI-SSL ersetzt das UMS Zertifikat: Wenn SonicWall DPI-SSL aktiviert ist, fungiert es als Zwischen-CA und sendet anstelle des ursprünglichen UMS Zertifikats ein eigenes Zertifikat an die Geräte. In der Folge weigern sich die Geräte, sich zu registrieren, weil sie nur das ursprüngliche UMS Zertifikat akzeptieren würden.

Lösung

1. Fügen Sie in SonicWall unter **DPI-SSL Status** die IP-Adresse des UMS Servers zur Liste der DPI-SSL-Ausnahmen hinzu.
2. Starten Sie den VPN-Tunnel neu.

Den Hostnamen eines Geräts über die IGEL UMS ändern

Es gibt zwei verschiedene Wege den Hostnamen eines Endgeräts über die IGEL Universal Management Suite (UMS) zu ändern:

Option 1:

Wenn **UMS-internen Namen anpassen, falls Netzwerkname geändert wurde** unter **UMS Konsole > UMS Administration > Globale Konfiguration > Geräte-Netzwerkeinstellungen** aktiviert ist:

Für IGEL OS 12:

1. Wählen Sie in der **UMS Web App > Geräte** das Gerät aus.
2. Wählen Sie **Konfiguration bearbeiten**.
3. Gehen Sie zu **Netzwerk > Allgemeine Einstellungen > Computername** und geben Sie den gewünschten Hostnamen an.
4. Speichern Sie die Einstellungen.
5. Wählen Sie aus, dass die Einstellungen **Sofort** übernommen werden sollen.
6. Aktualisieren Sie das Browserfenster, um den geänderten Hostnamen anzuzeigen.
7. Starten Sie das Gerät neu.

Für IGEL OS 11 und früher:

1. Klicken Sie in der **UMS Konsole > Geräte** mit der rechten Maustaste auf das Gerät.
2. Wählen Sie **Konfiguration bearbeiten**.
3. Gehen Sie zu **Netzwerk > LAN-Schnittstellen**.
4. Ändern Sie den **Terminalnamen**.
5. Klicken Sie **Speichern**.
6. Wählen Sie aus, dass die Einstellungen **Sofort** übernommen werden sollen.
7. Klicken Sie in der UMS auf **Aktualisieren**, um den geänderten Hostnamen anzuzeigen.
8. Starten Sie das Gerät neu.

Option 2:

Wenn **Netzwerknamen anpassen, falls UMS-interner Name geändert wurde** unter **UMS Konsole > UMS Administration > Globale Konfiguration > Geräte-Netzwerkeinstellungen** aktiviert ist:

1. Klicken Sie in der **UMS Konsole > Geräte** mit der rechten Maustaste auf das Gerät.
2. Wählen Sie **Umbenennen**.
3. Ändern Sie den Namen.
4. Klicken Sie **Ok**.
5. Klicken Sie mit der rechten Maustaste auf das Gerät.
6. Wählen Sie **Weitere Befehle > Einstellungen UMS -> Gerät**.
7. Starten Sie das Gerät neu.

Managing IGEL OS Devices by Device Specific Data - What Device Attributes Can Do for You

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

Start der UMS Konsole / Web App

UMS Web App: The Browser Displays a Security Warning (Certificate Error)

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

Das Starten der UMS Konsole stürzt die NX-Sitzung ab

Symptom

Wenn Sie über NX mit einem Ubuntu-Host verbunden sind, stürzt das Starten der UMS Konsole auf dem Ubuntu-Host die NX-Sitzung ab.

Lösung

1. Werden Sie **Root** im Ubuntu-Host.
2. Öffnen Sie die Konfigurationsdatei `/opt/IGEL/RemoteManager/rmclient/RemoteManager.bin.config` in einem Texteditor.
3. Fügen Sie die Zeile `vmparam -Dsun.java2d.xrender=false` zur Datei hinzu.
4. Speichern Sie die Datei.
5. Werden Sie regulärer Benutzer.
6. Starten Sie die UMS Konsole.

UMS Konsole startet nicht auf Linux-System ohne X11.

Symptom

IGEL UMS startet nicht auf Linux-System ohne X11.

Problem

Die UMS Konsolenanwendung benötigt X11, um ausgeführt zu werden.

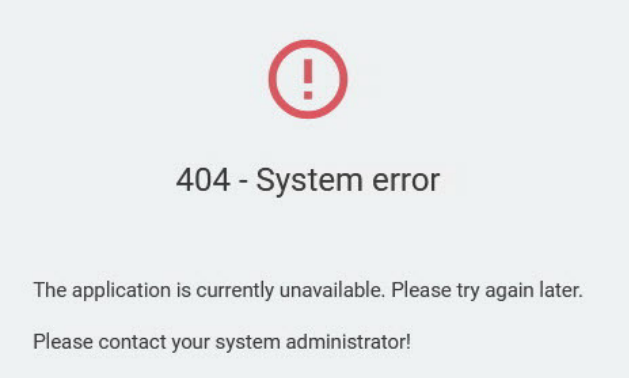
Lösung

- Installieren Sie X Window System (X11) um die IGEL UMS auszuführen.

UMS Web App: Fehlermeldung "404 - System Error"

Symptom

Nach der Installation von Universal Management Suite startet die UMS Web App mit einem 404-Systemfehler.



Umgebung

- UMS 6.08.100 oder höher mit der Embedded-Datenbank
- Microsoft Windows Server 2019

Problem

Dies kann beim Start passieren, wenn die UMS Web App schneller startet als der UMS Server-Dienst.

Lösung

▶ Starten Sie den Windows-Dienst `IGEL RMGUIServer` neu. Wie Sie das tun können, erfahren Sie unter IGEL UMS HA-Dienste und -Prozesse (see page 949).

Anmeldefehler

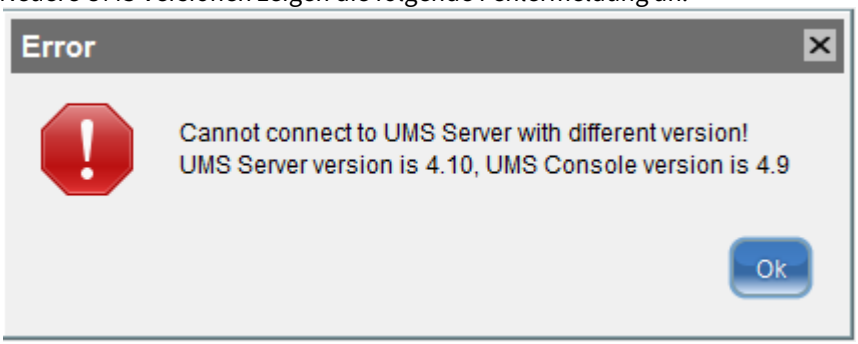
- Anmeldefehler in der UMS Konsole
- Die Anmeldung der UMS Konsole mit dem AD-Benutzerkonto schlägt fehl.
- Anmeldung an der UMS ist nach dem Update nicht möglich

UMS Konsolen Anmeldefehler

Symptom

Beim Versuch sich in der Konsole anzumelden erhalten Sie die Fehlermeldung **Der Baum konnte nicht geladen werden.**

Neuere UMS Versionen zeigen die folgende Fehlermeldung an:



Problem

Probleme mit der Verbindung zwischen der UMS Konsole und dem UMS Server können durch verschiedene Software Versionen verursacht werden, z. B. wenn der UMS Server aktualisiert wurde, die Konsole aber immer noch eine alte Version verwendet.

Lösung

Überprüfen Sie den Versionsstatus:

1. Überprüfen Sie die Version der Konsole, indem Sie im UMS Konsolenstrukturbaum **Hilfe > Info** wählen.
2. Überprüfen Sie die Version des Servers, indem Sie im UMS Administratormenü **Hilfe > Info** wählen.
3. Aktualisieren Sie bei Bedarf die UMS Konsole auf die gleiche Version wie der Server oder neuer.

Die Anmeldung der UMS Konsole mit dem AD-Benutzerkonto schlägt fehl.

Symptom

Die Anmeldung an der UMS Konsole schlägt für Active Directory-Benutzer fehl.

Problem

1. Catalina Logdatei öffnen `C:\Program Files\IGEL\RemoteManager\rmguiserver\logs\catalina.log`
2. Überprüfen Sie das Protokoll nach der Nachricht `KDC has no support for encryption type (14)`

Lösung

Wenn dies der Fall ist, müssen die folgenden Dinge durchgeführt/geprüft werden:

1. Werfen Sie einen Blick auf http://technet.microsoft.com/en-us/library/cc733991.aspx.
2. Deaktivieren Sie **DES encryption** für den AD Benutzer, dies kann in der Kontoeinrichtung der Windows-Benutzerverwaltung > Kontooptionen vorgenommen werden.
3. Folgen Sie http://docs.oracle.com/javase/6/docs/technotes/guides/security/jgss/tutorials/Troubleshooting.html.

Anmeldung an der UMS ist nach dem Update nicht möglich

Symptom

Sie können sich nach einem Update oder der Installation des UMS Servers nicht an der UMS anmelden.

Eine Fehlermeldung mit der URL `https://[ums_server_host]:8443/info` erscheint:

Problem

Der IGEL RMGUI Server Service ist noch nicht vollständig gestartet.

Lösung

Warten Sie noch ein paar Minuten. Versuchen Sie danach, sich erneut anzumelden.

Active Directory / LDAP

Active Directory integrieren

Problem

Anstatt UMS-Administratoren manuell zu erstellen und zu organisieren, suchen Sie nach einer einfachen Möglichkeit, sie aus Ihrem bestehenden Active Directory zu importieren.

Grund

Sie möchten Benutzer und Benutzergruppen aus dem Active Directory in das UMS importieren und dabei die gleichen AD-Gruppenzuordnungen und Anmeldeinformationen verwenden, die bereits im AD definiert sind.

Lösung

In diesem Beitrag erläutern wir die beste Methode, Benutzer aus dem Active Directory als UMS-Administratorkonten zu importieren.

Der Import von Benutzern aus dem Active Directory in die UMS-Konsole erfolgt in drei Schritten:

- Die Verbindung zum Active Directory konfigurieren
- Die zu importierenden Benutzer auswählen und den Import starten
- Berechtigungen zuweisen

- Das Konfigurieren einer AD-Verbindung (see page 184)
- Benutzerkonten vom AD in die UMS importieren (see page 187)
- Berechtigungen zuweisen (see page 190)
- Eine LDAP Verbindung konfigurieren (see page 194)

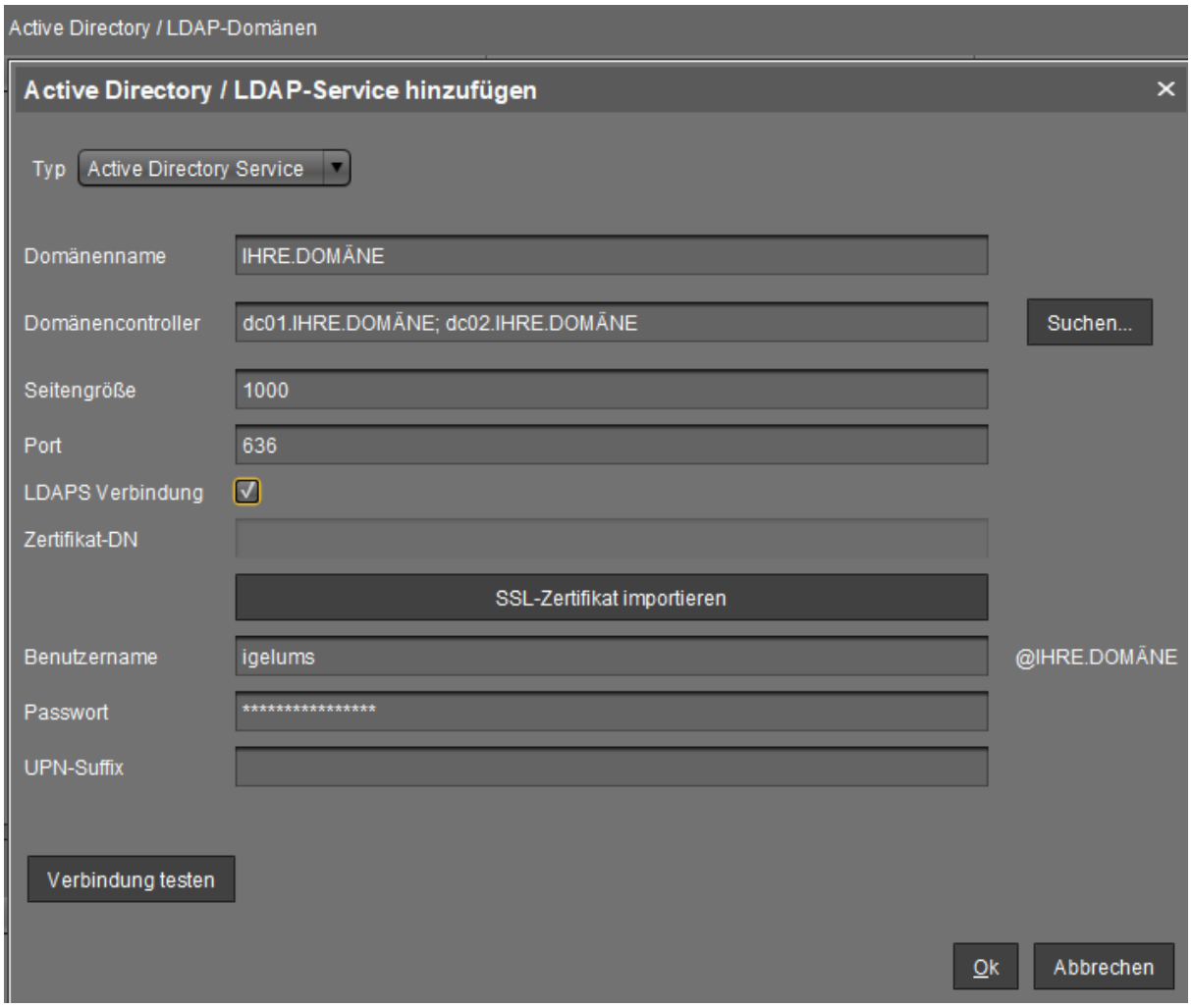
Das Konfigurieren einer AD-Verbindung

Führen Sie die folgenden Schritte aus, um die Verbindung zwischen der UMS und dem Active Directory Ihres Unternehmens herzustellen**.**

1. Wenn Sie Benutzer- und Gruppenabhängigkeiten zwischen verschiedenen konfigurierten Domänen/Subdomänen haben, möchten Sie vielleicht **Alle konfigurierten AD Domains für Suche und Import von AD Usern / Gruppen berücksichtigen** aktivieren. Mit dieser Option wird die Gruppensuche für einen Benutzer innerhalb aller konfigurierten Domänen aktiviert. Bei der Aktivierung wird ein Bestätigungsdialog angezeigt.

   > Wenn diese Option aktiviert ist, kann ein Benutzer zusätzliche Berechtigungen erhalten. Dies ist dann der Fall, wenn
   > - der Benutzer in einer Gruppe ist, die aufgrund dieser Option gefunden wurde,
   > - diese Gruppe unter **System > Administratorkonten** importiert wurde,
   > - und dieser Gruppe Berechtigungen zugewiesen wurden, d. h. Berechtigungen, die der Benutzer sonst nicht haben würde.
   >
   > Bitte beachten Sie, dass diese Option aufgrund der zusätzlichen Suchvorgänge Auswirkungen auf die Performance in den folgenden Bereichen haben kann:
   > - UMS-Anmeldung
   > - Berechtigungsdialoge
   > - Shared Workplace (SWP)

2. Klicken Sie auf **Hinzufügen (+)** unter UMS-Konsole > **UMS Administration > Globale Konfiguration** > **Active Directory / LDAP**.
   Der Dialog **Active Directory / LDAP-Service hinzufügen** öffnet sich.



3. Wählen Sie **Active Directory Service** als **Typ**.

4. Geben Sie den **Domänenname**n an.

   > Es lassen sich mehrere Active Directories anbinden. Achten Sie daher beim Einloggen, z. B. an der UMS Konsole, auf die Angabe der korrekten Domäne.

5. Geben Sie den/die **Domänencontroller** manuell an oder klicken Sie auf **Suchen...** für automatisches Ausfüllen.
   Um mehrere Domänencontroller voneinander zu trennen, verwenden Sie ein Semikolon.

   > Falls die Option **LDAPS Verbindung** (siehe unten) aktiviert ist, stellen Sie sicher, dass ein vollständiger Name vom **Domänencontroller** (FQDN) eingegeben wurde. Siehe Probleme bei der Konfiguration von Active Directory mit LDAPS (see page 196).

6. Geben Sie die **Seitengröße** an.
   Die **Seitengröße** legt die maximale Anzahl von Elementen auf jeder Seite der Ergebnisse fest, die

bei einer Suche zurückgegeben werden. Diese Eigenschaft beeinflusst die Performanz der Abfrage, aber nicht die Anzahl der Gesamtergebnisse. Der Standardwert ist "1000". Ändern Sie diesen Wert entsprechend Ihrer Serverkonfiguration.

7. Aktivieren Sie **LDAPS Verbindung**, um die Verbindung mit dem angegebenen Zertifikat zu sichern. Der Port ändert sich automatisch auf den Standardport "636".

8. Klicken Sie auf **SSL-Zertifikat importieren**, um das Zertifikat zu konfigurieren und den **Zertifikat-DN** zu verifizieren.

   > Da der Name des **Domänencontroller**s gegen das Zertifikat geprüft wird, müssen diese übereinstimmen.
   > Falls mehr als ein Domänencontroller verwendet wird, muss ein Stammzertifikat der Domäne konfiguriert werden. Siehe Probleme bei der Konfiguration von Active Directory mit LDAPS (see page 196).

   > Die unterstützten Zertifikatsformate sind `.cer`, `.pem` und `.der`

9. Geben Sie unter **Benutzername** und **Passwort** Ihre Benutzerdaten ein. Der Benutzer muss Lesezugang in Active Directory haben.

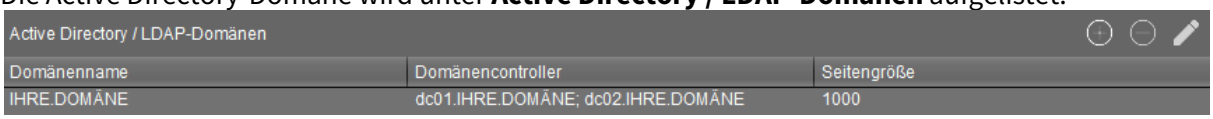
   > Achten Sie bei der Eingabe des Benutzernamens auf die Groß- und Kleinschreibung.

10. Geben Sie Aliase unter **UPN-Suffix** an, falls Sie sie konfiguriert haben (durch Semikolon getrennte Liste). Beispiel: `domain.local;test.local`

    > Die Einstellungen müssen der Konfiguration des Active Directory entsprechen. Wenn es im AD registrierte UPN-Suffixe gibt, sollten diese auch der UMS bekannt sein.

11. Klicken Sie auf **Verbindung testen**, um zu überprüfen, ob die richtige Konfiguration angegeben wurde.

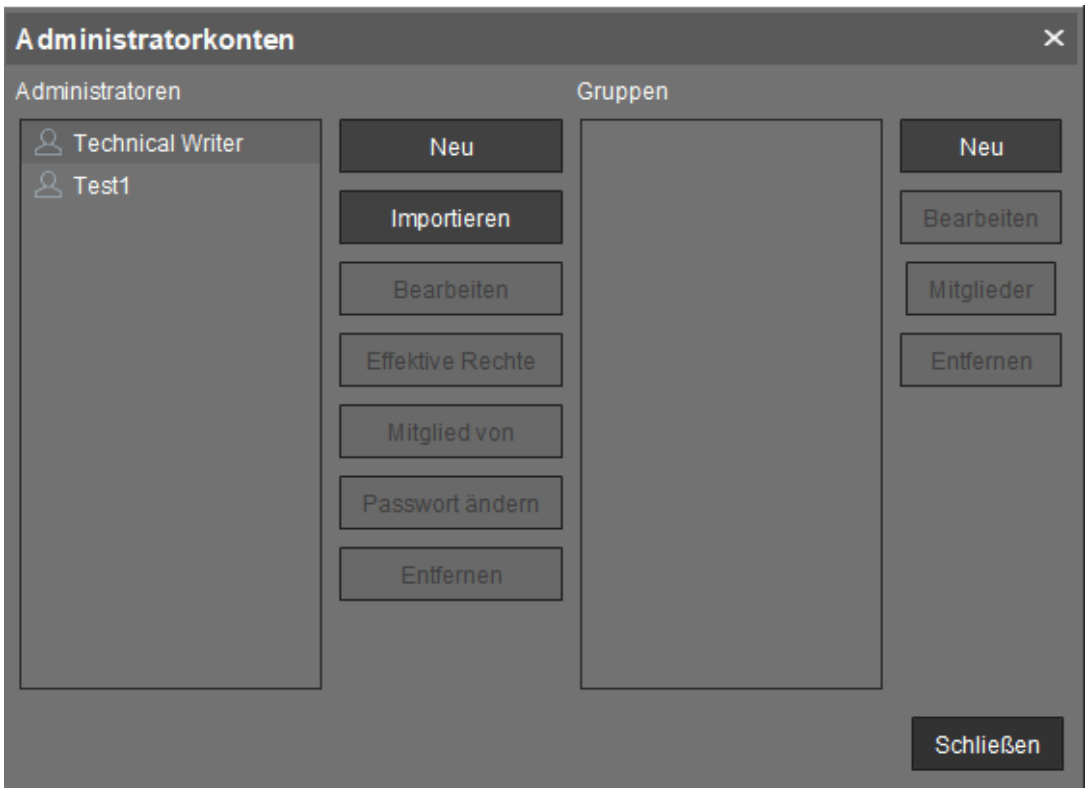
12. Klicken Sie auf **Ok**, um die Änderungen zu bestätigen.
    Die Active Directory-Domäne wird unter **Active Directory / LDAP-Domänen** aufgelistet.



Benutzerkonten vom AD in die UMS importieren

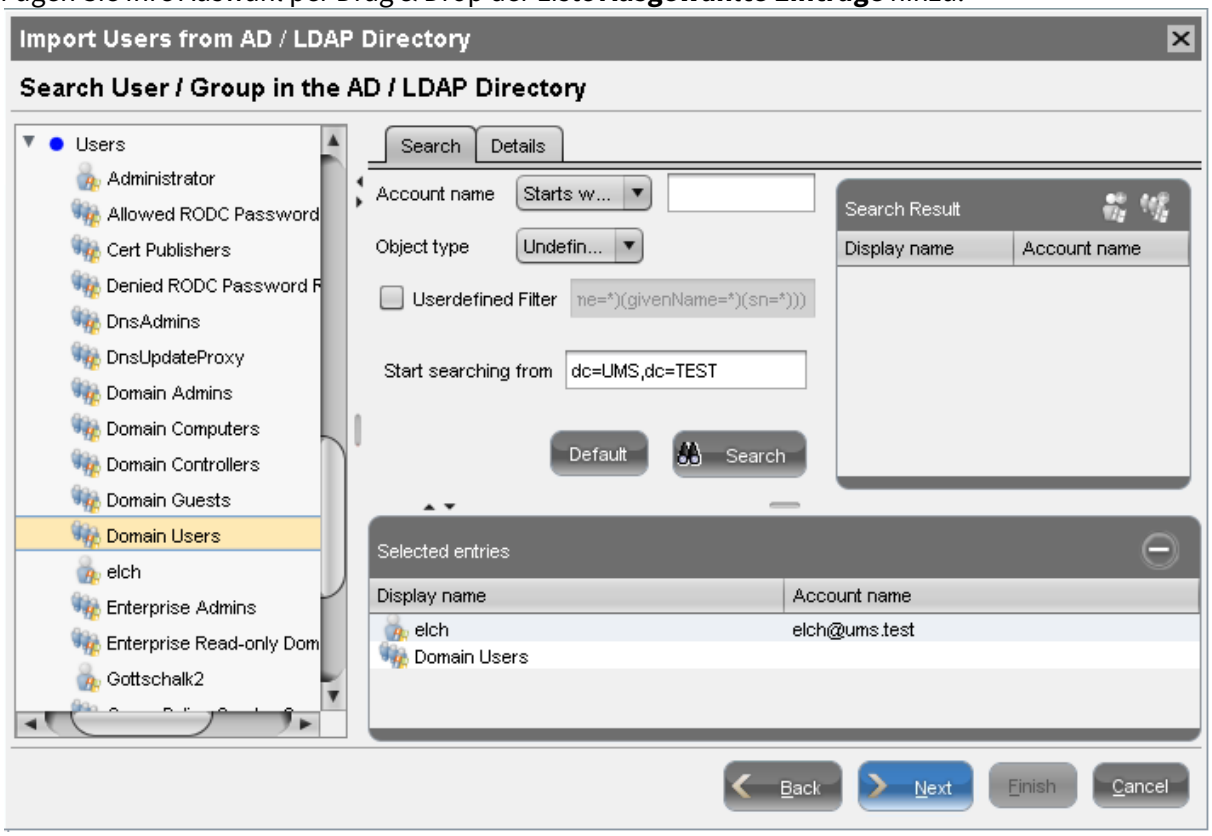
Nach der Verbindung mit dem Active Directory können Sie Konten von Benutzern oder Benutzergruppen in die UMS importieren:

1. Gehen Sie auf **System > Administratorkonten.**
   Das **Administratorkonten** Fenster öffnet sich:



2. Klicken Sie **Importieren,** um sich am AD/LDAP Service anzumelden.
3. Wählen Sie die Domäne aus und geben Sie Ihre Zugangsdaten ein, falls nicht bereits definiert.
4. Klicken Sie auf **Weiter,** um den Active Directory-Browser zu öffnen.
5. Wählen Sie einzelne Benutzer oder Gruppen aus dem Strukturbaum Ihres AD aus.

6. Fügen Sie Ihre Auswahl per Drag & Drop der Liste **Ausgewählte Einträge** hinzu.



> ⓘ Alternativ zur Navigation im Strukturbaum können Sie über die Suchfunktion auch Benutzer oder Gruppen zu Ihrer Auswahl hinzufügen.

7. Klicken Sie **Weiter** und bestätigen Sie den Import zu starten.
   Eine Ergebnisliste der importierten Konten wird geöffnet.

8. Klicken Sie **Fertig** um den Import zu vervollständigen.

Wenn die Ergebnisliste entweder leer ist oder Konten in der Liste fehlen, siehe Import von Administratorkonten aus dem Active Directory schlägt fehl (see page 198).

> Ein versehentlich eingerichteter UMS-Administrator muss manuell über den Dialog 'Administrator-Konten' gelöscht werden. Das IGEL UMS verwendet als Namen des importierten Benutzers den aus der AD stammenden 'User Logon Name'.

Berechtigungen zuweisen

Nachdem die AD-Benutzer importiert wurden, können sie mit ihren Active Directory-Anmeldeinformationen auf das UMS zugreifen.

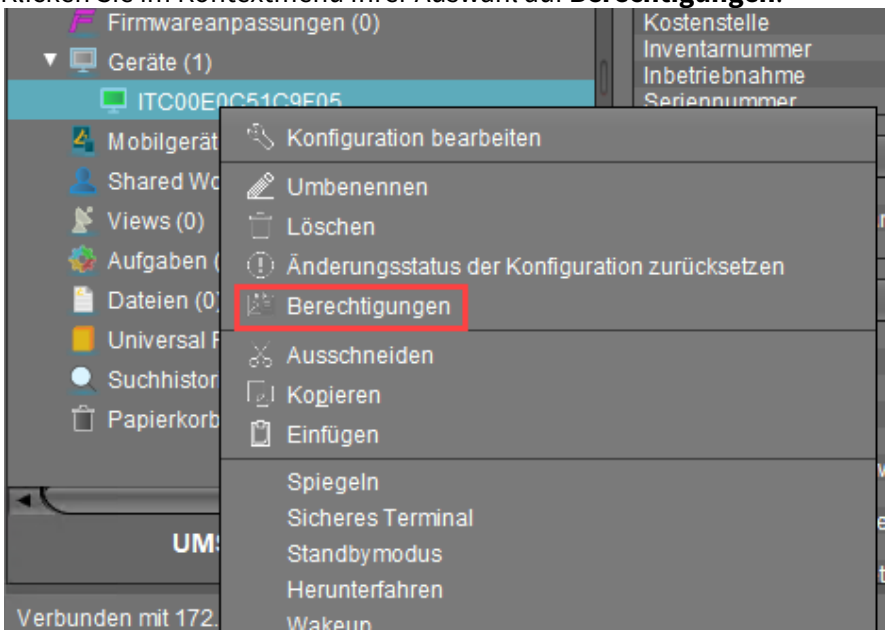
Als UMS-Administratoren benötigen die Benutzer weiterhin individuelle Zugriffsrechte.

> Die Anmeldung am UMS ist nicht über den 'pre Windows 2000 Anmeldenamen' ('DOMAIN\logon name') möglich, sondern nur über das Format 'logon name@DOMAIN'.

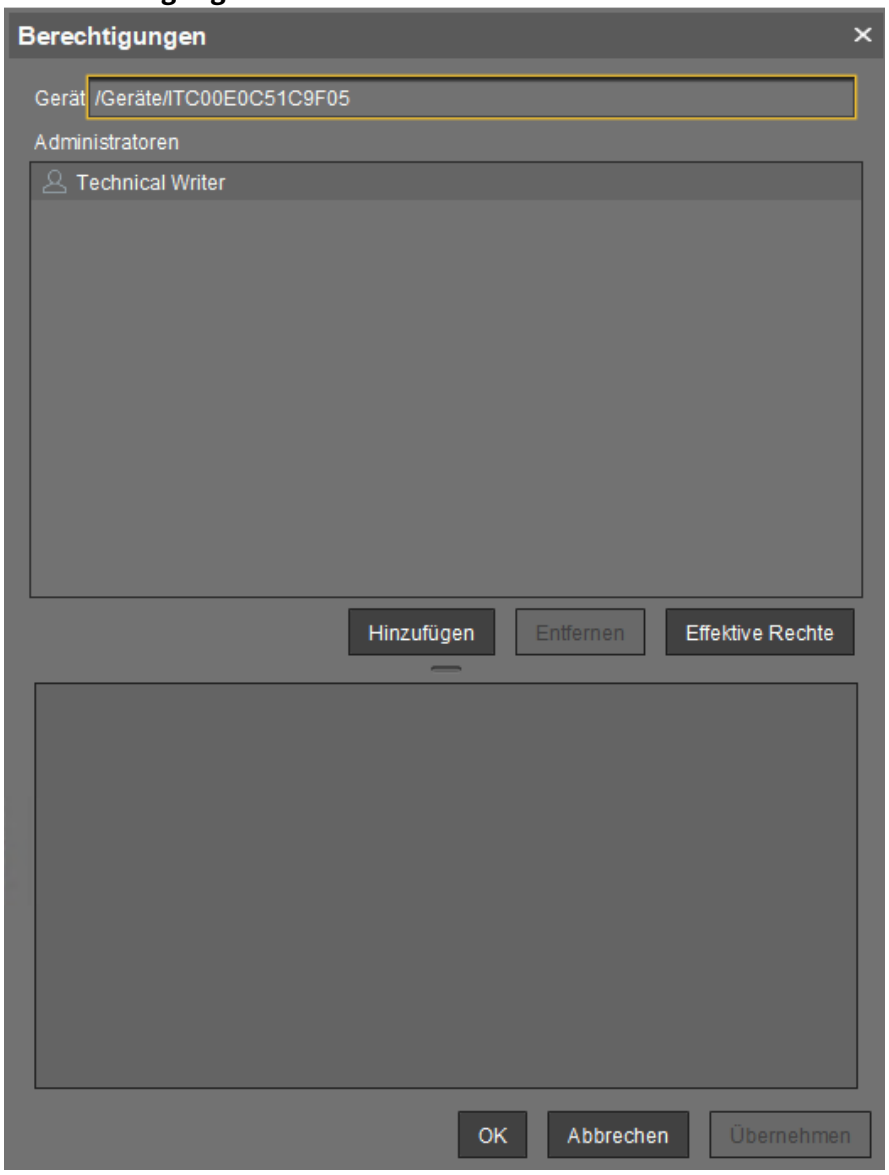
> Um beispielsweise die Konfiguration eines Gerätes ändern zu können, benötigt ein Benutzer die Berechtigung, den Verzeichnispfad des Gerätes zu durchsuchen und das Gerät selbst zu konfigurieren.

Um diese Rechte zu vergeben, gehen Sie wie folgt vor:

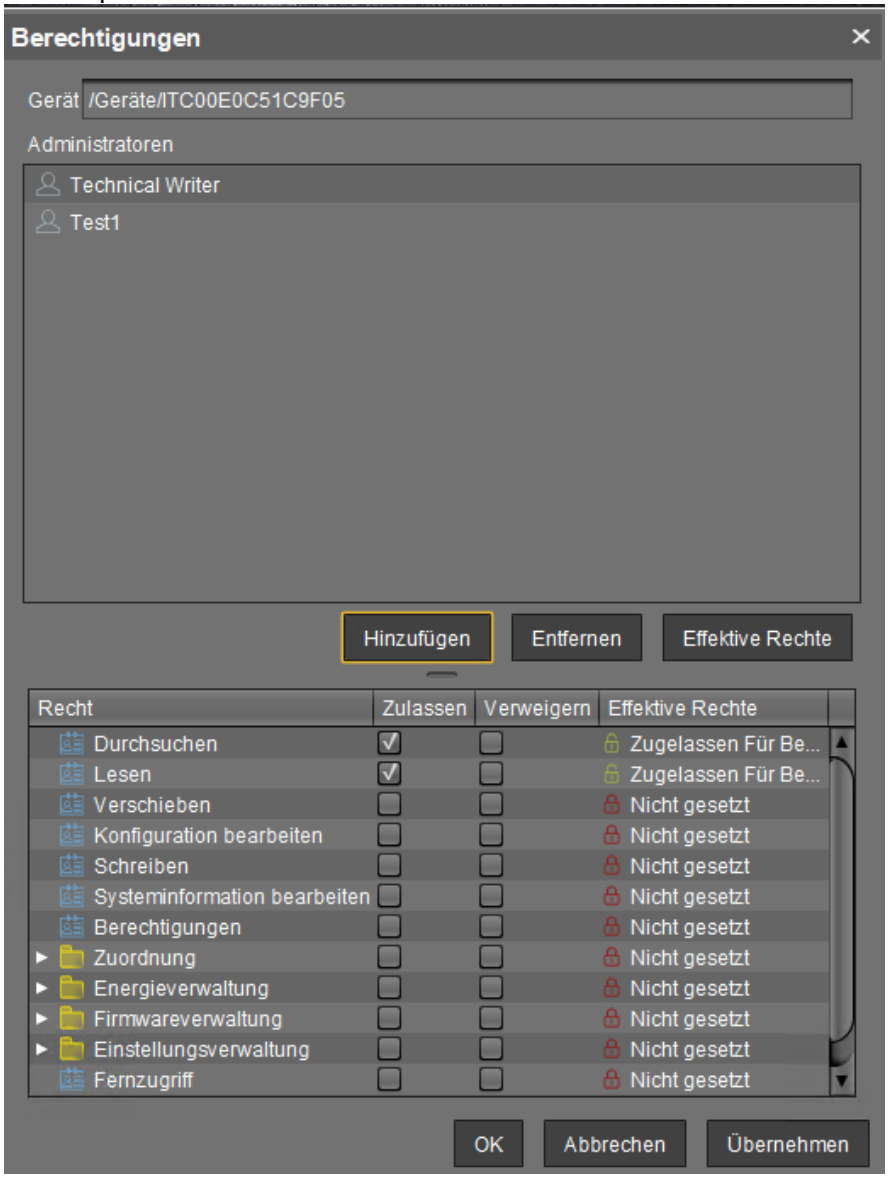
1. Wählen Sie im Strukturbaum der UMS-Konsole den Menüpunkt **Geräte** oder eine Untergruppe von Geräten oder ein einzelnes Gerät.
2. Klicken Sie im Kontextmenü Ihrer Auswahl auf **Berechtigungen**.



3. Das **Berechtigung**-Fenster öffnet sich.



4. Klicken Sie **Hinzufügen** um Ihren neuen Benutzer/Gruppe auszuwählen.
   Die entsprechenden effektiven Rechte werden im unteren Teil der Maske aufgelistet.



5. Sie können nun die Rechte der ausgewählten Gruppe oder des ausgewählten Benutzers für den Zugriff auf die ausgewählten Geräte **zulassen** oder **verweigern.**
6. Bestätigen Sie die Einstellungen mit **OK.**
7. Klicken Sie in der Konsole auf **Aktualisieren**, um die Änderungen in der UMS zu übernehmen.

> Wenn Sie die Rechte der registrierten Benutzer geändert haben, werden diese erst nach einer Aktualisierung wirksam.

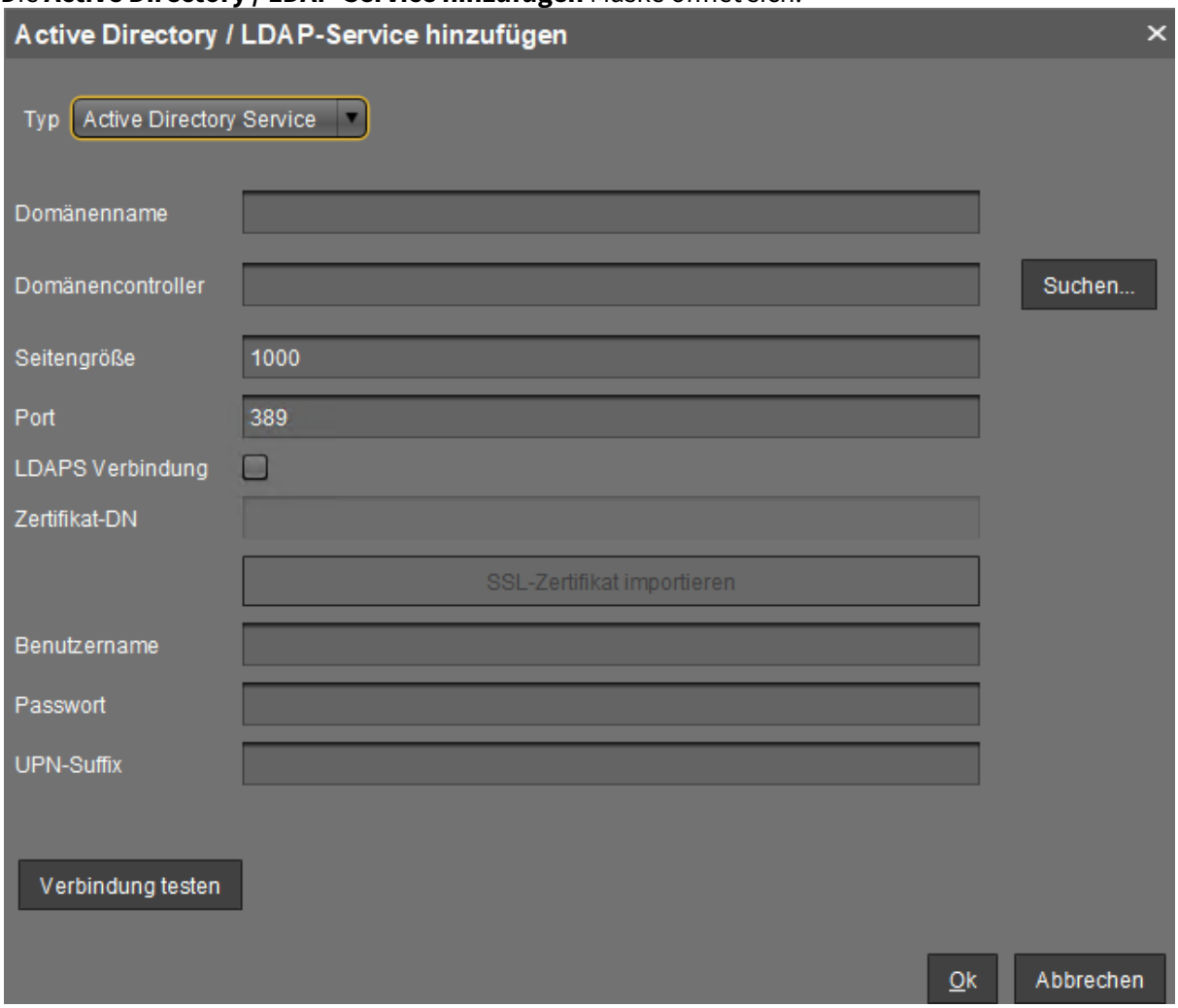
Weitere Details zu den Autorisierungsregeln finden Sie in unserem How-To Regeln für Benutzerautorisierung (see page 79).

Zugriffsrechte auf Objekte oder Aktionen innerhalb des IGEL UMS sind den Administratorkonten und -gruppen zugeordnet. Die Rechte des Datenbankbenutzerkontos können nicht eingeschränkt werden. Sie werden bei der Installation oder beim Einrichten der Datenquelle erstellt. Das Konto hat immer volle Zugriffsrechte im UMS.

Eine LDAP Verbindung konfigurieren

Als Variante können Sie andere LDAP-Verzeichnisdienste, z.B. Novell eDirectory und OpenLDAP, an die UMS anschließen:

1. Klicken Sie im Bereich **UMS Administration** der UMS-Konsole auf **Active Directory / LDAP**.
2. Klicken Sie unter **Active Directory / LDAP Domäne** auf **Hinzufügen (+)**.
3. Die **Active Directory / LDAP-Service hinzufügen** Maske öffnet sich.



4. Wählen Sie **Sonstiger LDAP-Service** als **Typ.**
5. Geben Sie den **Basis-DN** und den **LDAP-Benutzer-DN** gemäß dem LDAP Data Interchange Format ein.
6. Geben Sie die IP ihres Gerätes in das **Host(s)** Feld ein; bei mehreren Geräten verwenden Sie eine durch Kommas getrennte Liste.
7. Der Standard **Port** für LDAP über SSL ist 636.

> Aus Sicherheitsgründen unterstützt UMS nur sichere LDAP-Verbindungen.

8. Geben Sie unter **Benutzerpasswort** die Zugangsdaten für den LDAP Service Zugang ein. Der Benutzer muss über Leserechte für den gesamten Verzeichnisdienst verfügen, da er für die Bestimmung der Struktur im Verzeichnisdienst verwendet wird.
9. Geben Sie unter **Naming-Attribut** den Namen der LDAP-Attribute ein, der den eindeutigen Namen des Benutzerkontos enthält.
10. Fügen Sie optional einen **zusätzlichen Ausdruck für die LDAP-Suche** hinzu, der an die Suche nach Benutzern angehängt wird. Auf diese Weise kann die Leistung optimiert werden.
11. Geben Sie als **Gruppenattribut** den Namen des LDAP-Attributs ein, das die Gruppenzugehörigkeit eines Benutzers enthält.
12. Definieren Sie die **Seitengröße**. Diese Eigenschaft legt die maximale Anzahl von Elementen auf jeder Seite der Ergebnisse fest, die von einer Suche zurückgegeben werden. Es beeinflusst die Abfrageleistung, aber NICHT die Anzahl der Gesamtergebnisse. Der Standardwert ist 1000. Ändern Sie diesen Wert entsprechend Ihrer Serverkonfiguration.
13. Klicken Sie **SSL-Zertifikat importieren** um das Zertifikat DN zu überprüfen.

Probleme bei der Konfiguration von Active Directory mit LDAPS

Symptom

Sie können keine AD-Verbindung unter **Active Directory / LDAP** mit der aktivierten Option **LDAPS Verbindung** konfigurieren. Beim Testen der Verbindung erscheint einer der folgenden Arten von Fehlermeldungen:

- "`Verbindung zum LDAP-Server fehlgeschlagen! Überprüfen Sie den Servernamen und das Zertifikat`";
- "`simple bind failed`".
  Die Protokolldatei sieht so aus:
- "`2019-05-23 14:13:38,512 ERROR [https-jsse-nio-8443-exec-151] dec: simple bind failed: QA-DC01:636 javax.naming.CommunicationException: simple bind failed: QA-DC01:636 [Root exception is javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: No subject alternative DNS name matching QA-DC01 found.]`"
  oder
- "`javax.naming.CommunicationException: simple bind failed: dc01.your.domain:636 [Root exception is javax.net.ssl.SSLHandshakeException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target]`"

Problem

Der Name von **Domänencontroller** und das unter **SSL-Zertifikat importieren** konfigurierte Zertifikat stimmen nicht überein.

Lösung

1. Überprüfen Sie, ob ein *vollständiger Name des Domänencontrollers (FQDN)* eingegeben wurde, z. B. "dc01.ihre.domäne". Eine IP-Adresse oder ein Kurzname wie "dc01" wird nicht akzeptiert, wenn der Name des Domänencontrollers gegen das Zertifikat geprüft wird.
2. Falls mehr als ein Domänencontroller verwendet wird, stellen Sie sicher, dass das *Stammzertifikat* der Domäne konfiguriert wurde.

Import von Administratorkonten aus dem Active Directory schlägt fehl

Symptomimportieren

Der Import von UMS Administratoren aus einem Active Directory schlägt fehl, die Ergebnisliste der importierten Konten ist entweder leer oder es fehlen einige Konten in der Liste.

Problem

Active-Directory-Benutzerkonten können einen leeren User Principal Name (UPN) haben. Dies tritt auf, wenn ein älteres Active Directory (z. B. unter Windows NT 4.0) auf ein neues aktualisiert wird, indem die AD-Benutzerkonten auf das neue AD migriert werden.

Lösung

1. Stellen Sie die UPN für jedes zu importierende AD-Konto ein.
2. Wiederholen Sie den Import von AD Benutzern in die IGEL UMS.

Profile

Priorität eines Profils in der IGEL UMS herausfinden

Die Verwendung von Profilen ist eine sehr praktische Methode zur Verwaltung und Konfiguration von einem, zehn oder tausend Endgeräten mit der IGEL Universal Management Suite (UMS). Wenn Sie jedoch eine große Anzahl von Profilen bereitstellen, kann es verwirrend werden. Einige Profile haben möglicherweise überlappende Bereiche und versuchen daher, unterschiedliche Werte für einen bestimmten Parameter auf einem Gerät einzustellen. Ein Profil wird immer gewinnen, aber welches ist es? Glücklicherweise kann die UMS die Reihenfolge der Prioritäten auf einen Blick darstellen.

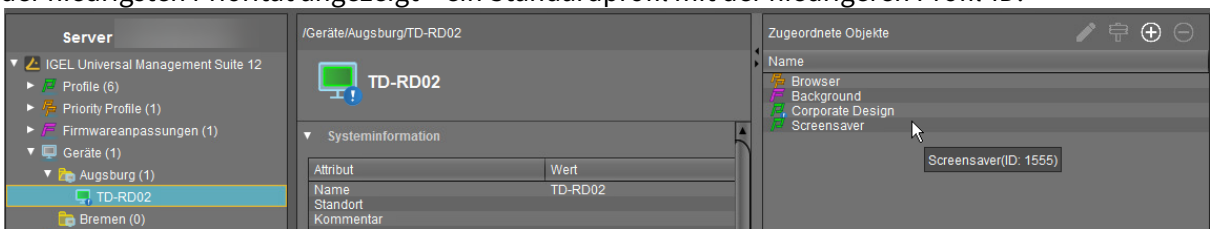
Eine umfassende Referenz der Profile finden Sie unter Profile in der IGEL UMS (see page 365); die Priorisierung wird in Priorisierung von Profilen in der IGEL UMS (see page 398) behandelt.

Das folgende Beispiel zeigt, wie Sie die Priorität eines Profils herausfinden können:

1. Wählen Sie in der **UMS Konsole > Geräte** das Gerät aus, für das Sie die Reihenfolge der Profilprioritäten sehen möchten.

2. Werfen Sie einen Blick in den Bereich **Zugeordnete Objekte**. Alle Profile, die dem Gerät zugeordnet sind, werden nach Priorität in absteigender Reihenfolge aufgelistet. Das Profil mit der höchsten Priorität wird zuerst aufgelistet, usw.

   Im folgenden Screenshot ist das Profil mit der höchsten Priorität ein sogenanntes Priority Profil. Danach folgt eine Firmwareanpassung, die wiederum eine höhere Priorität als ein Standardprofil hat, siehe Firmwareanpassungen in der IGEL UMS (see page 435). Und ganz unten wird das Objekt mit der niedrigsten Priorität angezeigt – ein Standardprofil mit der niedrigeren Profil-ID.



Vorrang von IGEL UMS Profilen und Universal Firmware Updates

Dieser Artikel erklärt, welche Einstellungen zum Firmwareupdate wirksam sind, wenn Ihrem IGEL OS Gerät mehrere konkurrierende Einstellungen zugewiesen sind. Einstellungen zum Firmwareupdate können lokal auf dem Gerät definiert sein, durch ein oder mehrere Profile, oder durch ein oder mehrere Universal Firmware Updates.

Allgemeine Rangfolge

Grundsätzlich ist die Rangfolge wie folgt, vom höchsten bis zum niedrigsten Rang:

- Universal Firmware Update
- Profil
- Lokale Einstellungen

Die Einzelheiten finden Sie in den nachfolgenden Abschnitten.

Universal Firmware Update gegen Profil

Wenn Ihrem Gerät ein Universal Firmware Update zugewiesen ist sowie ein Profil, das Einstellungen zum Firmwareupdate enthält, hat das Universal Firmware Update Vorrang gegenüber dem Profil. Dies gilt auch, wenn das Profil ein sogenanntes Priority Profil ist; weitere Informationen finden Sie unter Priorisierung von Profilen in der IGEL UMS (see page 398).

Die folgenden Einstellungen unter **System > Update > Firmwareupdate** werden von einem Universal Firmware Update überschrieben:

- **Protokoll**
- **Servername**
- **Port**
- **Pfadname auf dem Server**
- **Benutzername**
- **Passwort**

Profil gegen lokale Einstellungen

Die Einstellungen eines Profils überschreiben immer die lokalen Einstellungen.

Universal Firmware Update gegen Universal Firmware Update

Wenn einem einzigen Gerät mehrere Universal Firmware Updates zugewiesen sind, finden die unten beschriebenen Regeln Anwendung.

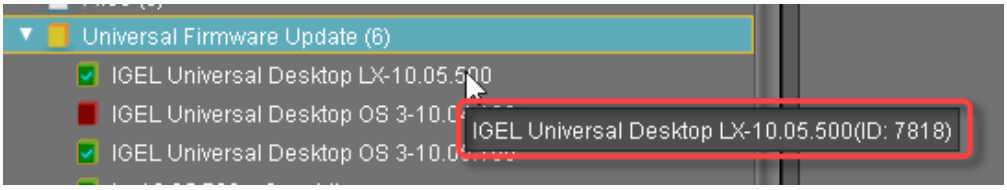
Zuweisung zu verschiedenen Ebenen in einer Ordnerhierarchie

Wenn einem Gerät über verschiedene Ordner und Unterordner mehrere Universal Firmware Updates zugewiesen sind, hat dasjenige Vorrang, das dem Gerät am nächsten steht.

Beispiel: Ein Universal Firmware Update für IGEL OS 10.05.100 ist einem Ordner namens "Geräte" zugewiesen, der unser Gerät enthält. Ein weiteres Universal Firmware Update, das IGEL 10.06.100 enthält, ist einem Ordner namens "teamA" zugewiesen. Der Ordner "teamA" enthält seinerseits den Ordner "Geräte".

Zuweisung auf der gleichen Ebene

Wenn mehrere Universal Firmware Updates auf der gleichen hierarchischen Ebene zugewiesen sind, hat das mit der höchsten ID Vorrang über die anderen. Um die ID eines Universal Firmware Updates zu finden, bewegen Sie den Mauszeiger über das betreffende Universal Firmware Update und lesen Sie den Tooltip:



In diesem Beispiel ist die ID 7818.

Kompatibilität

Nur die Universal Firmware Updates sind wirksam, die mit dem Gerät kompatibel sind.

Profile den Geräten zuweisen, die nach Ansicht oder Suche gefiltert sind.

Gültig für UMS Version 5.02.100 und höher.

Wenn Sie ein Profil einer Gruppe von Geräten zuordnen möchten, die ein bestimmtes Kriterium erfüllen, können Sie wie folgt vorgehen:

1. Definieren Sie eine Ansicht, die die Clients nach einem bestimmten Kriterium filtert (z. B. alle Geräte, die einen USB-Speicher-Hotplug enthalten).
2. Klicken Sie mit der rechten Maustaste auf die Ansicht um das Kontextmenü zu öffnen.
3. Klicken Sie **Objekte zu den Geräten der View zuordnen.**
   Das **Objekt zuordnen** Fenster öffnet sich.
4. Wählen Sie das relevante Profil aus (z. B. Das Profil, das USB-Speicher-Hotplug erlaubt).
5. Klicken Sie  um es von der linken in die rechte Spalte zu verschieben.
6. Bestätigen Sie die Einstellung mit **Ok.**

Ebenso können Sie Geräte eines Suchergebnisses Profile zuweisen:

1. Klicken Sie mit der rechten Maustaste auf die Ansicht um das Kontextmenü zu öffnen.
2. Klicken Sie **Objekte zu den Geräten der Suche zuordnen.**
   Das **Objekt zuordnen** Fenster öffnet sich.
3. Wählen Sie das relevante Profil aus und klicken Sie  um es von der linken in die rechte Spalte zu verschieben.
4. Bestätigen Sie die Einstellung mit **Ok.**

▶ Um die Profilzuordnung aufzuheben, klicken Sie auf **Profile von den Geräten der Ansicht trennen** oder **Suche.**

> Sie können den Ansichten oder Suchergebnissen auch automatisch und regelmäßig Profile als administrative Aufgabe zuordnen.

Troubleshooting: Profileinstellungen Werden Nicht Angewendet

Problem

Wenn ein IGEL Universal Management Suite (UMS)-Profil auf ein OS 11- oder OS 12-Gerät angewendet wird, werden einige Einstellungen des Profils nicht korrekt auf das Gerät übertragen.

Lösung

Durch Hinzufügen eines automatischen Neustarts zum UMS-Profil wird die korrekte Anwendung der Einstellungen aus dem Profil auf das Gerät sichergestellt.

So lösen Sie den automatischen Neustart aus, wenn das Profil auf das Gerät angewendet wird:

1. Gehen Sie im UMS-Profil zu **System > Firmwareanpassung > Eigene Befehle > Desktop**. Weitere Informationen zu eigene Befehlen finden Sie unter Eigene Befehle und Custom Commands.

2. Fügen Sie den folgenden Befehl als **Finaler Desktopbefehl** hinzu:
   if [! -f /wfs/.one_more_reboot_done] ; then touch /wfs/.one_more_reboot_done ; systemctl reboot ; fi

3. Speichern Sie das Profil.

Extras

Wo kann ich die IGEL UMS Logdateien finden?

Der folgende Artikel beschreibt, wo Sie die Protokolldateien der IGEL Universal Management Suite (UMS) finden und konfigurieren können.

Wie Sie die Protokollierung der Aktionen des UMS Benutzers und der von einem Gerät gestarteten Aktionen aktivieren können, erfahren Sie unter Logging (see page 661).

Wenn Sie IGEL OS 12-Geräte verwalten, siehe Debugging / How to Collect Log Files.

Wenn Sie UMS Protokolldateien für den IGEL Support benötigen, lesen Sie Supportinformationen speichern / Logdateien an den Support senden (see page 701).

UMS 12.01 oder höher

Um die Logging-Einstellungen für UMS 12.01 oder höher zu ändern, lesen Sie die Datei `README.md` unter `[IGEL Installationsverzeichnis]/RemoteManager/rmguiserver/logs`.

Wenn Sie die Logging-Konfiguration ändern, ist ein Neustart des UMS Servers nicht erforderlich.

UMS Server

`rmguiserver/logs` (Lesen Sie `rmguiserver/logs/README.md` für die Konfiguration der Protokolle)	
`stderr.log`	Fehlermeldung des Apache Tomcat Servers
`stdout.log`	Standardausgabe des Apache Tomcat Servers
`ums-api.log`	Protokollierung des API-Dienstes
`ums-server.log` (= `catalina.log` vor UMS 12) `ums-server-err.log`	Zentrale Protokolldatei für alle protokollierten Ereignisse
`device-connector.log` `device-connector-err.log`	Protokollierung von Device Connector

`ums-device-service.log` `ums-device-service-err.log`	Protokollierung der OS 12-Gerätefunktionalität
`ums-appproxy.log` `ums-appproxy-err.log`	Protokollierung von UMS as an Update Proxy (see page 889)
`rmguiserver/logs/ ums-server` (`rmguiserver/conf/logback.xml` - für die Konfiguration der Protokolle)	
`ums-server-msg.log`	Protokollierung des Apache ActiveMQ-Messaging (High Availability und Distributed UMS)
`ums-server-communication.log`	Protokollierung der Kommunikation mit der UMS Konsole oder den Geräten Editieren bei <!-- Logging of UMS communication -->
`ums-server-threaddump.log`	Periodische Protokollierung der Threads
`ums-server-icg-communication.log`	Protokollierung der Kommunikation mit dem ICG Editieren bei <!-- Logging of UMS communication -->
`ums-server-health.log`	Protokollierung der UMS HA Statusprüfung (see page 944)
`ums-server-monitoring.log`	Protokollierung der Leistungsaufzeichnung (see page 662) Editieren bei `<!-- Logging of monitoring data -->`; ersetzen Sie `INFO` durch `DEBUG`, um detaillierte Informationen zu jedem Methodenaufruf zu erhalten

Beispiel: Wo ist die Protokollierung für den UMS Server zu konfigurieren

Dies ist ein Beispiel für die Datei `rmguiserver/conf/logback.xml`, in der Sie die Logs für den UMS Server konfigurieren können, d. h. die Protokollierung ein- und ausschalten, den Scan-Zeitraum oder die Anzahl der Tage für die Protokollierungshistorie ändern, usw:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
-<configuration scanPeriod="60 seconds" scan="true" debug="false">
```

```
<!-- The length of logging history in days -->
```

```
<property value="30" name="logs.history"/>

<!-- The maximum size of one log file -->
<property value="100MB" name="logs.maxsize"/>

<!-- The maximum size of the history -->
<property value="1GB" name="logs.historysizecap"/>

<!-- Logging of monitoring data -->
<!-- Elevate to 'DEBUG' to see the individual calls -->
<property value="INFO" name="monitoring.level"/>

<!-- Logging of UMS communication -->
<!-- Set to 'ALL' to enable and 'OFF' to disable -->
<property value="OFF" name="server2console.level"/>
<property value="OFF" name="server2tc.level"/>
<property value="OFF" name="server2usg.level"/>
<property value="OFF" name="usg2server.level"/>
<property value="OFF" name="server2server.level"/>

<!-- Logging level of domain service -->
<!-- OFF, INFO, DEBUG, ERROR -->
<property value="WARN" name="domainservicelog.level"/>
<!-- The appenders -->
```

```
rmguiserver/logs/unifiedprotocol
```

`communication.log`	Protokollierung der Kommunikation zwischen dem Gerät und der UMS (eingehende und ausgehende Befehle) Editieren Sie `rmguiserver/webapps/device-connector/WEB-INF/classes/config/logback.xml`, um die Protokolle zu konfigurieren. Editieren bei `<!-- Logging of device communication -->`; ersetzen Sie `OFF` durch `INFO` für die Protokollierung von Befehlsköpfen oder durch `ALL` für die Protokollierung von Befehlsköpfen und Nutzdaten
`domain-service.log`	Zentrale Protokolldatei für alle Ereignisse in der Befehlsbehandlung Editieren Sie `rmguiserver/conf/logback.xml`, um die Protokolle zu konfigurieren. Editieren bei `<!-- Logging level of domain service -->`
`device-auth.log`	Protokollierung von Problemen bei Onboarding der Geräte und Geräteauthentifizierung

UMS Load Balancer

`umsbroker/etc/work/logs` (`umsbroker/etc/conf/logback.xml` - für die Konfiguration der Protokolle)	
`ums-broker.log`	Zentrale Protokolldatei für alle protokollierten Ereignisse
`ums-broker-msg.log`	Protokollierung der ausgetauschten Nachrichten
`ums-broker-health.log`	Protokollierung der UMS HA Statusprüfung (see page 944)

`ums-broker-monitoring.log`	Protokollierung der Leistungsaufzeichnung (see page 662) Editieren bei `<!-- Logging of monitoring data -->`; ersetzen Sie `INFO` durch `DEBUG`, um detaillierte Informationen zu jedem Methodenaufruf zu erhalten

UMS Watchdog

`umswatchdog/etc/work/logs` (`umswatchdog/etc/conf/logback.xml` - für die Konfiguration der Protokolle)	
`ums-watchdog.log`	Zentrale Protokolldatei für alle protokollierten Ereignisse
`ums-watchdog-msg.log`	Protokollierung der ausgetauschten Nachrichten
`ums-watchdog-health.log`	Protokollierung der UMS HA Statusprüfung (see page 944)

UMS Konsole

`$HOME/.igel`	
`RMClient.exe.log`	Startprotokollierung
`$HOME/.igel/logs` (`rmclient/logback.xml` - für die Konfiguration der Protokolle)	
`ums-console.log`	Zentrale Protokolldatei für alle protokollierten Ereignisse

UMS Administrator

`$HOME/.igel`	
`RMAdmin.exe.log`	Startprotokollierung
`rmguiserver/logs` (`rmadmin/logback.xml` - für die Konfiguration der Protokolle)	
`ums-admin.log`	Zentrale Protokolldatei für alle protokollierten Ereignisse

UMS 6.10.110 und höher

In UMS Version 6.10.110 wurde das veraltete Logging-Framework Log4j 1.x durch Logback[8] ersetzt; siehe auch ISN 2022-19: Log4j 1.x Remainder in UMS.

Um die Logging-Einstellungen für UMS 6.10.110 oder höher zu ändern, verwenden Sie `logback.xml`.

UMS Server

`rmguiserver/logs` (`rmguiserver/conf/logback.xml` - für die Konfiguration der Protokolle)	
`catalina.log`	Zentrale Protokolldatei für alle protokollierten Ereignisse
`ums-server-msg.log`	Protokollierung des Apache ActiveMQ-Messaging
`ums-server-communication.log`	Protokollierung der Kommunikation mit der UMS Konsole oder den Gerä Editieren bei `<!-- Logging of UMS communication -->`
`localhost.log`	Technische Protokollierung des Apache Tomcat Servers
`stderr.log`	Fehlermeldung des Apache Tomcat Servers
`stdout.log`	Standardausgabe des Apache Tomcat Servers
`ums-server-threaddump.log`	Periodische Protokollierung der Threads
`ums-server-icg-communication.log`	Protokollierung der Kommunikation mit dem ICG Editieren bei `<!-- Logging of UMS communication -->`
`ums-server-health.log`	Protokollierung der UMS HA Statusprüfung (see page 944)
`ums-server-monitoring.log`	Protokollierung der Leistungsaufzeichnung (see page 662) Editieren bei `<!-- Logging of monitoring data -->`; ersetz `DEBUG`, um detaillierte Informationen zu jedem Methodenaufruf zu erh des Servers ist dann erforderlich)

Beispiel: Wo ist die Protokollierung für den UMS Server zu konfigurieren

8 https://logback.qos.ch/

Dies ist ein Beispiel für die Datei `rmguiserver/conf/logback.xml`, in der Sie die Logs für den UMS Server konfigurieren können, d. h. die Protokollierung ein- und ausschalten, den Scan-Zeitraum oder die Anzahl der Tage für die Protokollierungshistorie ändern, usw:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration debug="false" scan="true" scanPeriod="60 seconds">

<!-- General settings -->


<!-- Logging of monitoring data -->
<!-- Elevate to 'DEBUG' to see the individual calls -->
<property name="monitoring.level" value="INFO" />

<!-- Logging of UMS communication -->
<!-- Set to 'ALL' to enable and 'OFF' to disable -->
<property name="server2console.level" value="OFF" />
<property name="server2tc.level" value="OFF" />
<property name="server2usg.level" value="OFF" />
<property name="usg2server.level" value="OFF" />

<!-- The base folder for log files -->
<property name="base.dir" value="${catalina.home}/logs" />

<!-- The default logging pattern -->
<property name="pattern.format" value="%-5(%d{[yyyy-MM-dd HH:mm:ss.SSS]})
%-5level [%thread] %logger{10}.%M - %msg%n" />

<!-- The length of logging history in days -->
<property name="logs.history" value="30" />


<!-- The appenders -->
```

`rmguiserver/logs` (`rmguiserver/conf/logback.xml` - für die Konfiguration der Protokolle)	
`ums-api.log`	Protokollierung des API-Dienstes

UMS Load Balancer

`umsbroker/etc/work/logs` (`umsbroker/etc/conf/logback.xml` - für die Konfiguration der Protokolle)	
`ums-broker.log`	Zentrale Protokolldatei für alle protokollierten Ereignisse
`ums-broker-msg.log`	Protokollierung der ausgetauschten Nachrichten
`ums-broker-health.log`	Protokollierung der UMS HA Statusprüfung (see page 944)
`ums-broker-monitoring.log`	Protokollierung der Leistungsaufzeichnung (see page 662) Editieren bei `<!-- Logging of monitoring data -->` ; ersetzen Sie `INFO` durch `DEBUG` , um detaillierte Informationen zu jedem Methodenaufruf zu erhalten (ein Neustart des Servers ist dann erforderlich)

UMS Watchdog

`umswatchdog/etc/work/logs` (`umswatchdog/etc/conf/logback.xml` - für die Konfiguration der Protokolle)	
`ums-watchdog.log`	Zentrale Protokolldatei für alle protokollierten Ereignisse
`ums-watchdog-msg.log`	Protokollierung der ausgetauschten Nachrichten
`ums-watchdog-health.log`	Protokollierung der UMS HA Statusprüfung (see page 944)

UMS Konsole

`$HOME/.igel`	
`RMClient.exe.log`	Startprotokollierung
`$HOME/.igel/logs` (`rmclient/logback.xml` - für die Konfiguration der Protokolle)	
`ums-console.log`	Zentrale Protokolldatei für alle protokollierten Ereignisse

UMS Administrator

`$HOME/.igel`	
`RMAdmin.exe.log`	Startprotokollierung
`rmguiserver/logs` (`rmadmin/logback.xml` - für die Konfiguration der Protokolle)	
`ums-admin.log`	Zentrale Protokolldatei für alle protokollierten Ereignisse

Vor UMS 6.10.110

UMS Server

`rmguiserver/logs` (`rmguiserver/conf/log4j.properties` - für die Konfiguration der Protokolle)	
`catalina.log`	Zentrale Protokolldatei für alle protokollierten Ereignisse
`ums-server-msg.log`	Protokollierung des Apache ActiveMQ-Messaging
`communication.log`	Protokollierung der Kommunikation mit der UMS Konsole oder den Geräten Editieren bei `# communication logging - define the log levels` ; siehe Log4j-Dokumentation[9]
`license_deployment.log`	Lizenzprotokollierung Editieren bei `# license deployment logging` ; siehe Log4j-Dokumentation[10]
`localhost.log`	Technische Protokollierung des Apache Tomcat Servers
`stderr.log`	Fehlermeldung des Apache Tomcat Servers
`stdout.log`	Standardausgabe des Apache Tomcat Servers

9 https://logging.apache.org/log4j/2.x/manual/index.html
10 https://logging.apache.org/log4j/2.x/manual/index.html

`umsthreaddump.log`	Periodische Protokollierung der Threads Editieren bei `# threaddump logging` ; siehe Log4j-Dokumentation[11]
`usgcommunication.log`	Protokollierung der Kommunikation mit dem ICG Editieren bei `# communication logging - define the log levels` ; siehe Log4j-Dokumentation[12]
`health.log`	Protokollierung der UMS HA Statusprüfung (see page 944)
`monitoring.log`	Protokollierung der Leistungsaufzeichnung (see page 662) Editieren bei `# execution monitoring` ; ersetzen Sie `INFO` durch `DEBUG` , um detaillierte Informationen zu jedem Methodenaufruf zu erhalten (ein Neustart des Servers ist dann erforderlich)

`rmguiserver/logs` (`rmguiserver/conf/log4japi.properties` - für die Konfiguration der Protokolle)	
`api.log`	Protokollierung des API-Dienstes

UMS Load Balancer

`umsbroker/etc/work/logs` (`umsbroker/etc/conf/log4j.properties` - für die Konfiguration der Protokolle)	
`igel-ums-broker.log`	Zentrale Protokolldatei für alle protokollierten Ereignisse
`broker-msg.log`	Protokollierung der ausgetauschten Nachrichten
`broker-health.log`	Protokollierung der UMS HA Statusprüfung (see page 944)
`broker-monitoring.log`	Protokollierung der Leistungsaufzeichnung (see page 662) Editieren bei `# monitoring logging` ; ersetzen Sie `INFO` durch `DEBUG` , um detaillierte Informationen zu jedem Methodenaufruf zu erhalten (ein Neustart des Servers ist dann erforderlich)

11 https://logging.apache.org/log4j/2.x/manual/index.html
12 https://logging.apache.org/log4j/2.x/manual/index.html

UMS Watchdog

`umswatchdog/etc/work/logs` (`umswatchdog/etc/conf/log4j.properties` - für die Konfiguration der Protokolle)	
`igel-ums-watchdog.log`	Zentrale Protokolldatei für alle protokollierten Ereignisse
`watchdog-msg.log`	Protokollierung der ausgetauschten Nachrichten
`watchdog-health.log`	Protokollierung der UMS HA Statusprüfung (see page 944)

UMS Konsole

`$HOME/.igel`	
`RMClient.exe.log`	Startprotokollierung
`$HOME/.igel/logs` (`rmclient/log4j.properties` - für die Konfiguration der Protokolle)	
`igel-ums-console.log`	Zentrale Protokolldatei für alle protokollierten Ereignisse

UMS Administrator

`$HOME/.igel`	
`RMAdmin.exe.log`	Startprotokollierung
`rmguiserver/logs` (`rmadmin/log4j.properties` - für die Konfiguration der Protokolle)	
`igel-ums-admin.log`	Zentrale Protokolldatei für alle protokollierten Ereignisse

Clearing stdout.log and stderr.log in IGEL UMS

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

UMS bereinigen

Problem

Sie haben mehrere Firmware-Versionen in der UMS. Ihre Sammlung von Kunden und Profilen ist groß und verwirrend geworden. Sie verlieren den Überblick über Zuordnungen und Verbindungen zwischen diesen Elementen.

Ziel

Sie möchten die Vielfalt an Firmware und Profilen minimieren, um Prozesse zu vereinfachen. Sie wollen nur angezeigt bekommen, was sie wirklich benötigen.

Firmware, Geräte und Profile sind voneinander abhängig. Also, was ist der beste Weg, um vorzugehen?

Lösung

> Wir empfehlen, ein Backup der UMS zu erstellen, bevor Sie Komponenten löschen. Sie können auch den UMS Papierkorb für die gelöschten Objekte verwenden.

Im Folgenden werden die wichtigsten Schritte zur Reorganisation der UMS beschrieben:

1. Laden Sie die neue Firmware herunter.
2. Verschieben Sie die Geräte auf die neue Firmware.
3. Verschieben Sie Profile auf die neue Firmware.
4. Löschen Sie alte Firmware, Geräte und Profile, die nicht mehr benötigt werden.

Die neue Firmware herunterladen

1. Überprüfen Sie auf unserem download server[13], ob es neue Updates gibt, die für Ihre Anwendungen relevant sind.
2. Laden Sie die relevante Update-Datei herunter. Installieren Sie ein Update-Verzeichnis für die Dateien auf dem UMS-Server oder auf Ihrem FTP-Server.

Geräte auf die neue Firmware verschieben

Finden Sie heraus, wie viele verschiedene Firmware-Versionen Sie wirklich benötigen.

Aktualisieren aller Clients auf die gleiche Firmware:

1. Erstellen Sie eine neue **View**, um nach allen Clients zu suchen, die eine ältere Firmware Version als die aktuelle Version verwenden.
   Beispiel:
   View Name: Zeigt alle UD LX Geräte mit alter Firmware

13 https://www.igel.com/software-downloads/

Regel: Der Produktname ist wie (!reg!)(?i).*Universal Desktop LX.* AND Firmware Version ist älter als 5.04.100

2. Ordnen Sie diesen Geräten das Update-Verzeichnis zu.
3. Starten Sie den Updateprozess.

Profile auf neue Firmware verschieben

Überprüfen Sie Ihre Profile und entscheiden Sie, welche davon für die neue Firmware relevant sind. Sie haben drei Möglichkeiten, die Sie jetzt nutzen können:

- Passen Sie die Firmware-Version an, auf der die Profile basieren, um sicherzustellen, dass sie mit der neuen Firmware funktionieren.
- Lassen Sie die Profileinstellungen so, wie sie sind.
  Wenn die Parameter der neuen Firmware mit den Parametern der alten Version übereinstimmen, funktioniert ein Profil trotzdem. Wenn sie nicht übereinstimmen, werden diese Parameter ignoriert.
- Erstellen Sie neue Profile.

Mehr Informationen finden Sie im UMS Handbuch: Profile in der IGEL UMS erstellen (see page 372).

Alte Firmware, Clients und Profile löschen, die nicht mehr benötigt werden.

Um die UMS endgültig zu bereinigen, sollten Sie nun veraltete Objekte löschen.

- Verwenden Sie erneut Views, um die Clients auszuwählen, die nicht mehr benötigt werden.
  Weitere Informationen finden Sie im UMS Handbuch: Wie erstelle ich eine neue View in der IGEL UMS? (see page 490).
- Wählen Sie die obsoleten Profile aus. Sie können dies manuell oder über die Suchfunktion tun: **Extras > Suche > Profile > Produkt & Firmware.**
- Löschen Sie die alte Firmware, die nicht mehr einem Client oder Profil zugeordnet ist: **Exras > unbenutzte Firmwares entfernen.**

Haben Sie auch veraltete Views, Aufgaben, Template Keys? Löschen Sie sie auch.

UMS Zertifikat vom OS 11 Gerät entfernen

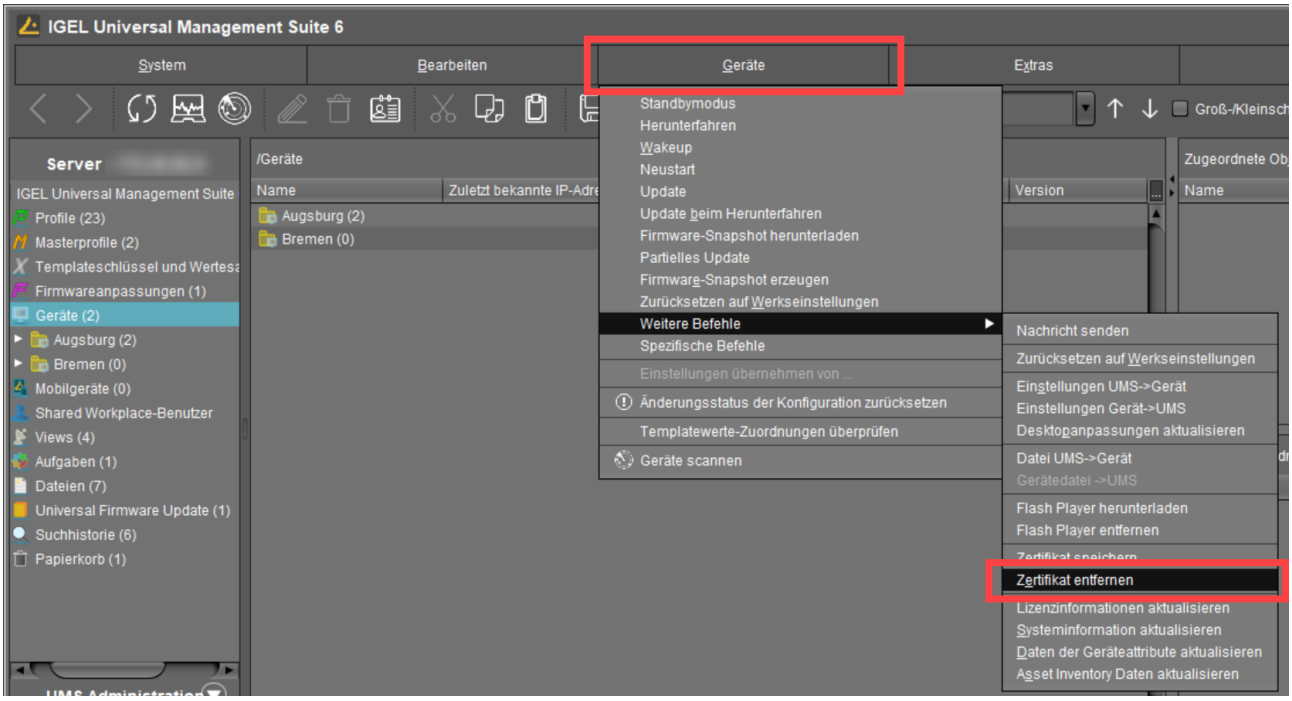
Die IGEL Universal Management Suite (UMS) sieht die Möglichkeit vor, das UMS Server-Zertifikat von OS 11 Geräten zu entfernen.

Die Entfernung des Zertifikats von Geräten kann erforderlich sein

- um den Umzug eines Geräts aus der Test- in die Produktivumgebung vorzubereiten
- um den Austausch des Serverzertifikats vorzubereiten

So entfernen Sie das Zertifikat:

▶ Gehen Sie auf **Geräte > Weitere Befehle** und wählen Sie **Zertifikat entfernen** aus.
Nun kann jeder IGEL UMS Server auf die Gerätekonfiguration zugreifen, bis einer der Server das Gerät registriert.



Ähnliche Themen

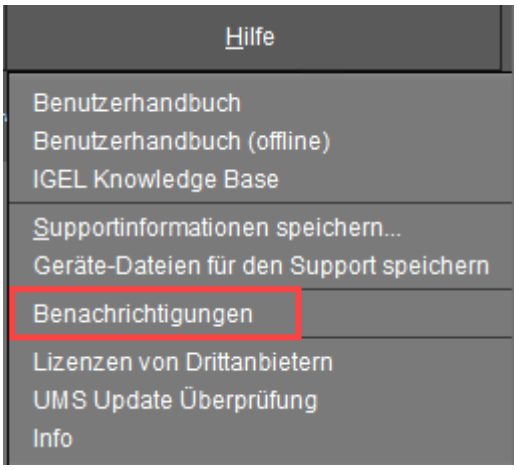
Wenn Sie bei der Geräteregistrierung auf Fehler wegen Zertifikatsproblemen stoßen: Troubleshooting: Die Registrierung eines Geräts über Suche nach Geräten schlägt fehl (see page 165)

Benachrichtigungen in der IGEL UMS konfigurieren

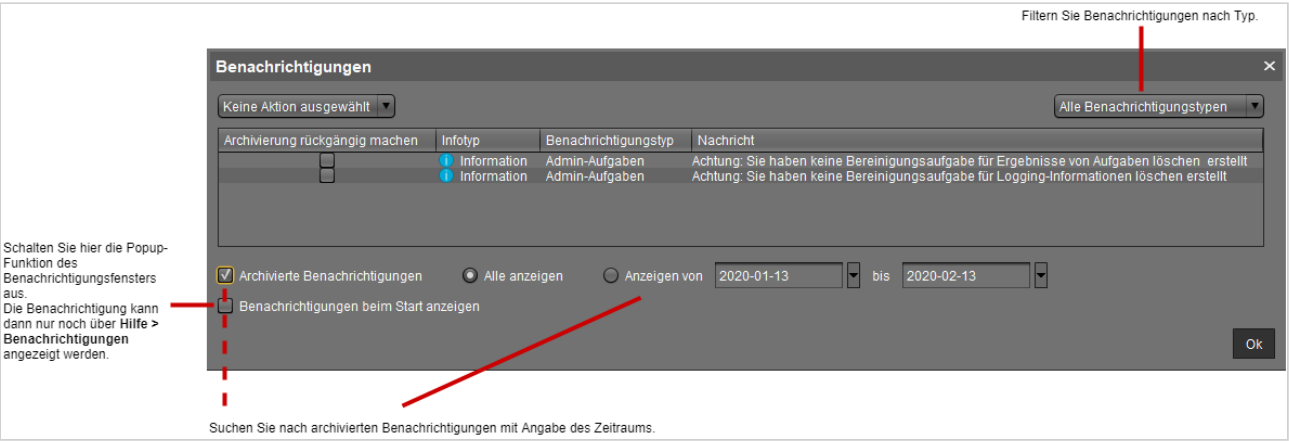
In der IGEL Universal Management Suite (UMS) können Sie Benachrichtigungen über neu verfügbare Firmwareupdates, Gerätelizenzen usw. erhalten. Standardmäßig sind die Benachrichtigungen aktiviert und erscheinen, wenn Sie die UMS Konsole starten. In diesem Artikel erfahren Sie, wie Sie diese Funktion an Ihre Bedürfnisse anpassen können.

Über Benachrichtigungen

Grundsätzlich können alle Benutzer mit Leseberechtigung die Benachrichtigungen sehen. Die Benachrichtigungen werden nach dem Start der UMS Konsole angezeigt. Wenn der Dialog geschlossen ist, können die Benachrichtigungen weiterhin jederzeit unter **Hilfe > Benachrichtigungen** eingesehen werden.



Das Benachrichtigungsfenster



Die Benachrichtigungsfunktion aktivieren

1. Gehen Sie in der UMS Konsole zu **UMS Administration > Globale Konfiguration > Zusätzliche Einstellungen**.
2. Aktivieren Sie **Benachrichtigungen aktivieren**.

Die Benachrichtigungsfunktion ist aktiv. Die Benachrichtigungen können unter **Hilfe > Benachrichtigungen** eingesehen werden.

Benachrichtigungen exportieren und per E-Mail versenden

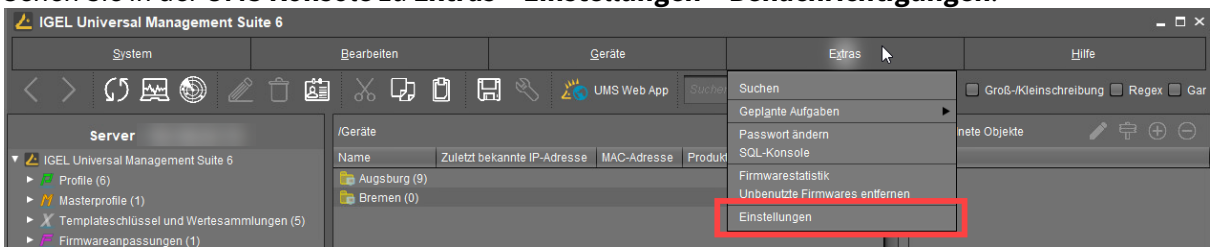
Die Benachrichtigungen können exportiert und per E-Mail versendet werden: **UMS Administration > Globale Konfiguration > Administrative Aufgaben > Hinzufügen > Aktion: "Sende Benachrichtigungen via E-Mail"**.

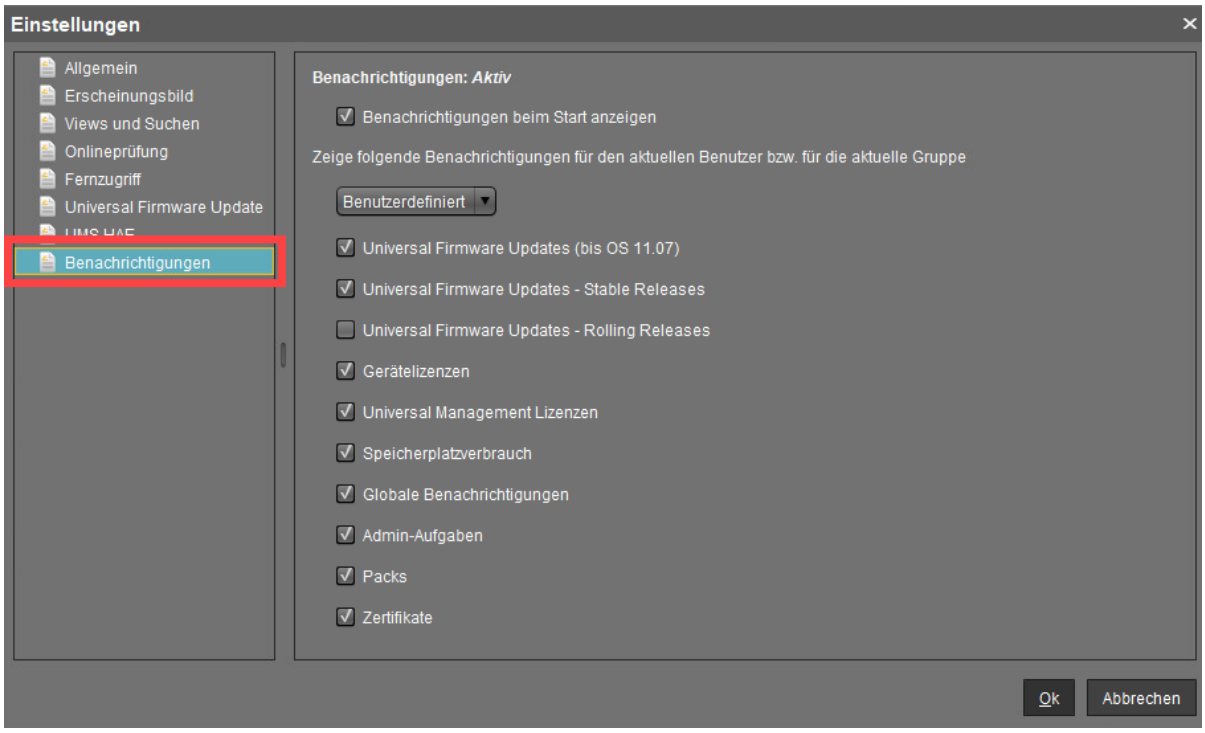
Mehr Informationen finden Sie unter Administrative Aufgaben - Zeitlich geplante Aktionen für die IGEL UMS konfigurieren (see page 597).

Popup-Benachrichtigung und Benachrichtigungstypen konfigurieren

Um das Benachrichtigungsfenster zu konfigurieren:

1. Gehen Sie in der **UMS Konsole** zu **Extras > Einstellungen > Benachrichtigungen**.





2. Aktivieren Sie **Benachrichtigung beim Start anzeigen**, um das Benachrichtigungsfenster bei jedem Start der UMS Konsole als Popup-Fenster anzuzeigen.

3. Wählen Sie **Benutzerdefiniert** unter **Zeige folgende Benachrichtigungen für den aktuellen Benutzer bzw. für die aktuelle Gruppe** aus.

4. Geben Sie an, welcher Inhalt in der Benachrichtigung angezeigt werden soll.
   Mögliche Optionen (ab UMS 6.10.110):
   - **Universal Firmware Updates (bis OS 11.07)**: Informiert über die neuesten Firmwareupdates für Geräte mit IGEL OS Versionen vor 11.07.

     > Um Benachrichtigungen anzuzeigen, die von UMS Versionen vor 6.10.110 generiert wurden, lassen Sie die Funktion **Universal Firmware Updates (bis OS 11.07)** aktiviert.

   - **Universal Firmware Updates - Stable Releases**: Informiert über die neuesten Stable Releases. Die Funktion wird offiziell für Geräte mit IGEL OS Version 11.07 oder höher unterstützt.
   - **Universal Firmware Updates - Rolling Releases**: Informiert über die neuesten Rolling Releases. Die Funktion wird offiziell für Geräte mit IGEL OS Version 11.07 oder höher unterstützt.

     > Aktivieren Sie diese Funktion, um die neuesten Versionen von Clients und Bug Fixes zu erhalten.

   - **Gerätelizenzen**: Informiert über den Ablauf von Gerätelizenzen.

- **Universal Management Lizenzen**: Informiert über den Ablauf von UMS Lizenzen und bei Überschreitung der Lizenzmenge.
- **Speicherplatzverbrauch**: Informiert über einen kritischen Wert des freien Festplattenplatzes. Für weitere Informationen siehe unten "Speicherplatzverbrauch".
- **Globale Benachrichtigungen**: Informiert über wichtige Neuigkeiten wie Maintenance-Termine und Bugfixes. Für weitere Informationen siehe unten "Globale Benachrichtigungen".
- **Admin-Aufgaben**: Informiert automatisch in einer Reihe von Fällen, wenn keine administrative Aufgabe festgelegt wurde. Für weitere Informationen siehe unten "Admin-Aufgaben".
- **Packs**: Informiert über den Ablauf von Lizenz-Packs.
- **Zertifikate**: Informiert über den Ablauf von Zertifikaten.

5. Bestätigen Sie die Einstellungen mit **Ok**.

Speicherplatzverbrauch

Diese Benachrichtigung informiert den Benutzer, wenn zu wenig freier Festplattenspeicher zur Verfügung steht. Der individuelle kritische Wert für den Speicherplatz kann unter **UMS Administration > Globale Konfiguration > Zusätzliche Einstellungen > Benachrichtigungen** eingestellt werden.

> Jeder Server führt im 6-Stunden-Rhythmus eine Admin-Aufgabe aus, um den verfügbaren Speicherplatz auf dem Laufwerk zu überprüfen und die Informationen zur Festplattennutzung an das Benachrichtigungssystem zu liefern. Eine Voraussetzung für die Anzeige der Benachrichtigung ist, dass der Server bis zu 6 Stunden kontinuierlich betrieben wurde.
> Ausführungen von Admin-Aufgaben, die älter als 24 Stunden sind, gelten als veraltet: Es wird eine zusätzliche Warnmeldung angezeigt.

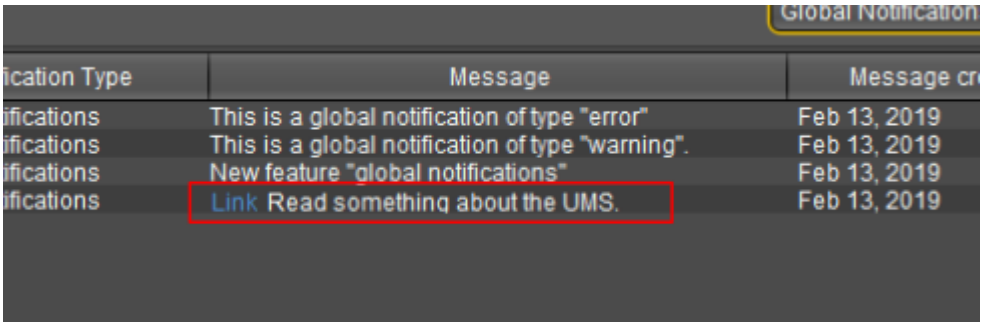
Arten von Benachrichtigungen über die Festplattennutzung:

- Spezifische Benachrichtigung für jeden angeschlossenen Server: Der Hostname des Servers und der verfügbare Speicherplatz werden in der Benachrichtigung angezeigt.
- Installationspfad und Datenbankpfad liegen auf verschiedenen Dateisystemen: Es werden zwei Benachrichtigungen für jedes Dateisystem angezeigt.

Globale Benachrichtigungen

Diese Benachrichtigungsart informiert den Benutzer über wichtige Neuigkeiten wie Maintenance-Termine und Bugfixes.

Globale Benachrichtigungen können einen zusätzlichen Weblink enthalten, der weitere Informationen liefern kann. Der Weblink wird als blaue Link-Schaltfläche neben der globalen Benachrichtigung angezeigt.



- ▶ Klicken Sie auf den Link, um die Webseite im Standardbrowser zu öffnen.
- ▶ Bewegen Sie die Maus über den Link, um die URL anzuzeigen.

Admin-Aufgaben

Benachrichtigungen dieses Typs werden in den folgenden Fällen angezeigt:

- Wenn eine Embedded-Datenbank aktiv ist, aber KEINE administrative Aufgabe zum **Erstellen einer Datenbanksicherung** erstellt wurde.
- Wenn Logging (see page 661) aktiviert ist, aber KEINE administrative Aufgabe zum **Löschen der Logging-Informationen** erstellt wurde.
- Wenn mindestens eine Aufgabe (see page 518) konfiguriert wurde, aber KEINE administrative Aufgabe zum **Löschen von Aufgaben-Ergebnissen** erstellt wurde.

Nähere Informationen zu administrativen Aufgaben finden Sie unter Administrative Aufgaben - Zeitlich geplante Aktionen für die IGEL UMS konfigurieren (see page 597).

Zeitzoneninformationen aktualisieren (Sommerzeit, Winterzeit)

Symptom

Der Thin Client zeigt eine falsche Tageszeit für Ihren Standort an, obwohl Sie die richtige Zeitzone eingestellt haben.

Problem

Die Zeitzone oder die Regelung für die Sommerzeit für Ihren Standort hat sich geändert.

Lösung

Aktualisieren Sie die Zeitzonen-Informationsdatei über die IGEL Universal Management Suite (UMS). Dies funktioniert jedem Fall für:

- IGEL Linux Version 10.01.100 oder neuer
- IGEL Linux Version 5.04.100 oder neuer
- IGEL Linux Version 4.14.100 oder neuer
- IGEL Linux ARM Version 1.09.100 oder neuer.

Abrufen der aktuellen Zeitzonen-Informationsdateien:

Auf Windows

- Verwenden Sie den Web Browser um die folgenden Paketdateien herunter zu laden:
  - http://packages.ubuntu.com/xenial-updates/all/tzdata/download für IGEL Linux Version 10.x
  - http://packages.ubuntu.com/trusty-updates/all/tzdata/download (für IGEL Linux Version 5.x)
  - http://packages.ubuntu.com/precise-updates/all/tzdata/download (für IGEL Linux Version 4.x)
- Entpacken Sie den Lieferumfang mit dem Programm 7-Zip. (frei verfügbar auf http://www.7-zip.org[14]).
- Suchen Sie die Datei für Ihren Standort im extrahierten Verzeichnis in `usr/share/zoneinfo/`, z. B. `usr/share/zoneinfo/Africa/Casablanca` für Marokko.

Auf Linux

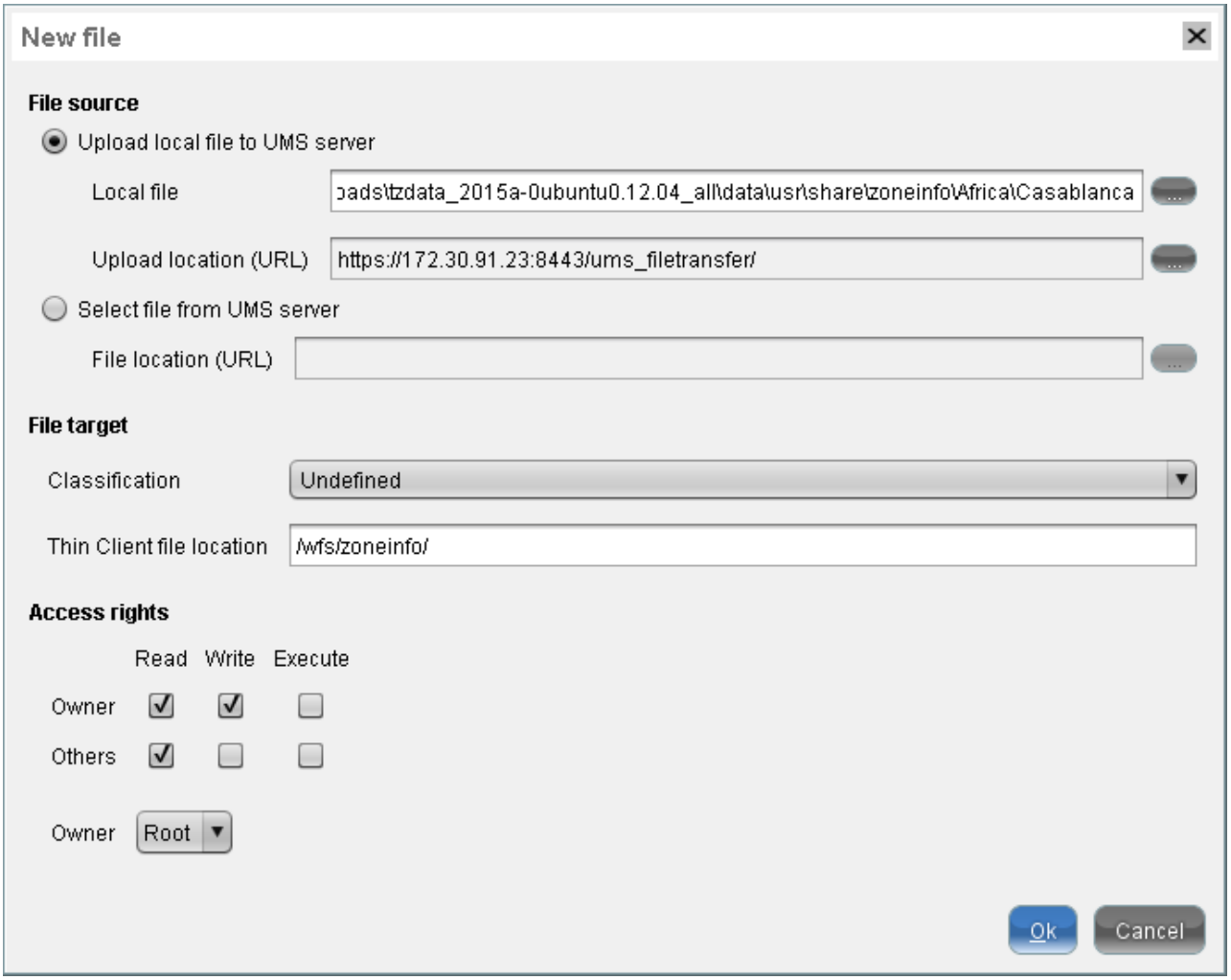
- Aktualisieren Sie Ihre System Zeitzoneninformation mit diesen Befehlen: `sudo apt-get updatesudo apt-get install tzdata`

14 http://www.7-zip.org/

- Suchen Sie die Datei für Ihren Standort im Systemverzeichnis `/usr/share/zoneinfo/` , z. B. `/usr/share/zoneinfo/Africa/Casablance` für Marokko.

Verteilung der Dateien aus der IGEL Universal Management Suite

- Wählen Sie **System > Neu > Neue Datei** in der Menüleiste der UMS Konsole oder gehen Sie auf **Dateien** im Strukturbaum und wählen Sie **Neue Datei** im Kontextmenü.
- Wählen Sie die Zeitzonen-Datei für Ihren Standort unter **Lokale Datei**.
- Wählen Sie **Nicht definiert** unter **Klassifizierung.**
- Spezifizieren Sie `/wfs/zoneinfo/` als **Speicherort für Thin Client Datei.**
- Setzen Sie die **Zugriffsrechte** auf Lesen und Schreiben für den Besitzer und Lesen für Andere.
- Wählen Sie Root als **Benutzer.**
- Klicken Sie **Ok** um die Einstellungen zu bestätigen.



Auf einem Thin Client können Sie die Übertragung und Aktivierung der neuen Zeitzonen-Informationsdateien überprüfen:

- Geben Sie im **lokalen Terminal** Folgendes ein: `grep 'timezone_config' /var/log/messages`

  > Auf IGEL Linux Version 10.x, verwenden Sie: `journalctl | grep 'timezone_config'.`

- Die Ausgabe sollte wie folgt aussehen:
  `Feb 27 11:28:13 (none) timezone_config: loading /wfs/zoneinfo/Casablanca to /usr/share/zoneinfo/Africa/Casablanca`
  `Feb 27 11:28:13 (none) timezone_config: loading /wfs/zoneinfo/Casablanca to /usr/share/zoneinfo/posix/Africa/Casablanca`
  `Feb 27 11:28:13 (none) timezone_config: configure timezone Africa/Casablanca`

E-Mail-Einstellungen für Gmail-Konten

Ziel

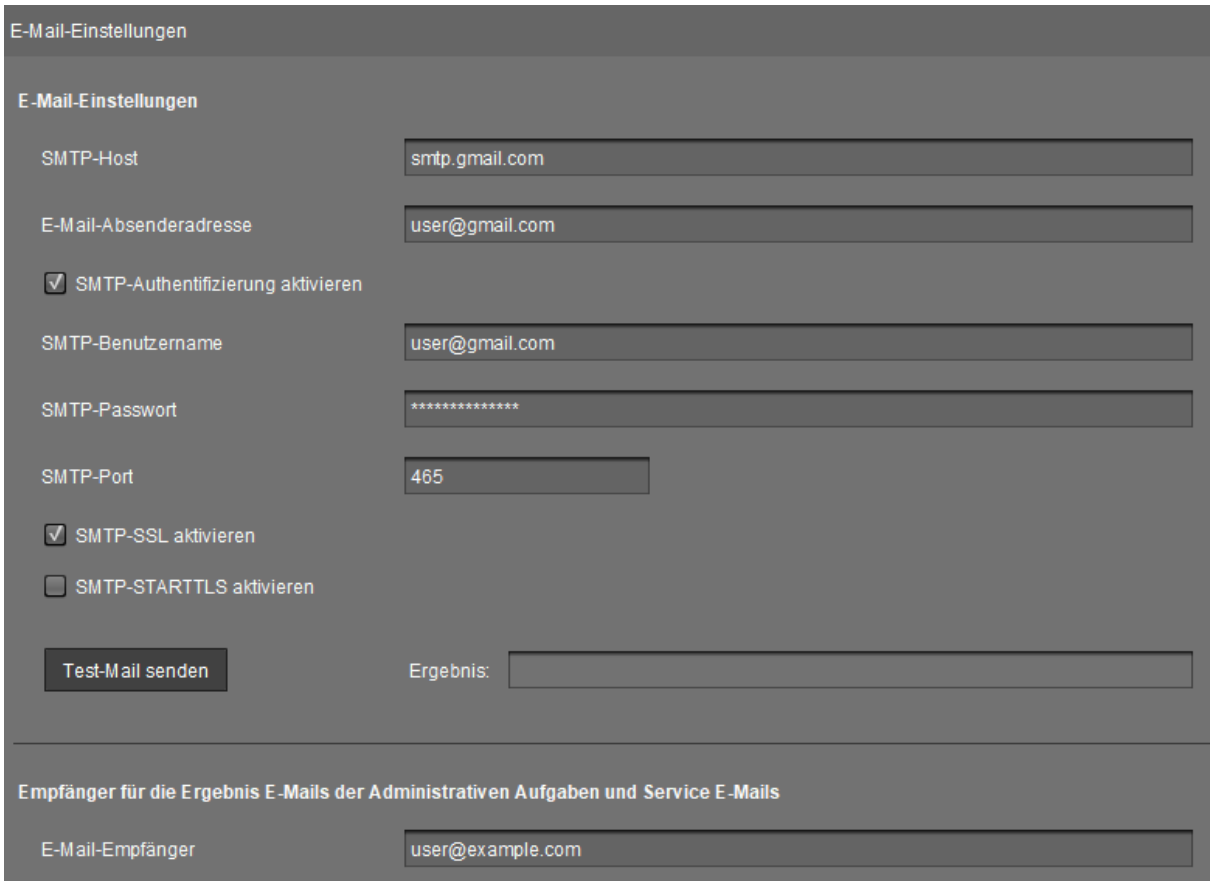
Sie möchten Views aus der IGEL Universal Management Suite über ein Gmail-Konto per E-Mail versenden.

Lösung

Damit die UMS Mails über Google Mail versenden kann, müssen Sie die folgenden Einstellungen in Ihrem Google-Konto vornehmen:

- Melden Sie sich bei Google an.
- Gehen Sie unter **Google-Konto verwalten > Sicherheit.**
- Setzen Sie **Zugriff durch weniger sichere Apps** auf `AN`.

1. Gehen Sie unter **UMS Administration > Globale Konfiguration > E-Mail-Einstellungen.**
2. Geben Sie `smtp.gmail.com` unter **SMTP-Host** ein.
3. Geben Sie Ihre Gmail-Adresse unter **E-Mail-Absenderadresse** an.
4. Setzen Sie einen Hacken bei **SMTP-Authentifizierung aktivieren.**
5. Geben Sie Ihre Gmail-Adresse unter **SMTP-Benutzername** an.
6. Geben Sie Ihr Gmail-Passwort unter **SMTP-Passwort** ein.
7. Geben Sie `465` unter **SMTP-Port** ein.
8. Aktivieren Sie nur **SMTP-SSL aktivieren.**
9. Geben Sie unter **E-Mail-Empfänger** die Adresse an, an die die administrativen E-Mails aus der UMS gesendet werden sollen.



10. Klicken Sie auf **Test-Mail senden,** um Ihre Einstellungen zu testen.

Zusätzliche Information

https://support.google.com/a/answer/176600?hl=en

Mit regulären Ausdrücken in der UMS suchen

Die Universal Management Suite (UMS) kann Ihnen bei der Verwaltung großer Thin Client-Installationen helfen. Häufig werden Sie nach Objekten mit bestimmten Eigenschaften suchen oder filtern wollen, und die UMS bietet eine große Auswahl. Für die erweiterte Suche benötigen Sie jedoch möglicherweise reguläre Ausdrücke, eine leistungsstarke Funktion von UMS.

Du kannst sie verwenden:

- Schnellsuche
- **Extras > Suche**
- **Views > Neue Views**
- **Bearbeiten > Konfiguration bearbeiten > System > Registry > Parametersuche...**
- **UMS Administration > Globale Konfiguration > Vorgabeverzeichnisse.**

UMS verwendet Java Regular Expressions. Diese unterscheiden sich von den Globbing-Mustern, die Sie vielleicht von der DOS/Windows-Eingabeaufforderung oder der Linux-Kommandozeile kennen. Anstatt beispielsweise * zu verwenden, um eine beliebige Anzahl von Zeichen abzugleichen, verwenden Sie in der UMS:

.*

Hier entspricht der . einem beliebigen Zeichen. Der * wirkt wie ein Quantisierer und gibt an, wie oft das vorhergehende Muster auftreten kann, in diesem Fall gar nicht oder mehrmals.

Wenn Sie also etwas finden möchten, das mit IGEL beginnt, verwenden Sie:

```
IGEL.*
```

Etwas, das mit IGEL beginnt und mit 12 endet:

```
IGEL.*12
```

Wenn Sie etwas finden wollen, das mit IGEL endet:

```
.*IGEL
```

Weitere Informationen zu Java Regular Expressions finden Sie in der Oracle's documentation[15].

15 https://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html

Sitzungen im Setup oder in der UMS kopieren

Manchmal möchten Sie eine Sitzung erstellen, die sich nur in wenigen Details von der anderen unterscheidet. IGEL Linux Version 5.10.100 oder neuer und UMS Version 5.02.100 oder neuer, ermöglichen Ihnen komplette Sitzungen zu kopieren. Nach dem Kopieren der Sitzung können Sie die erforderlichen Einstellungen einfach anpassen.

Das Kopieren ist im Abschnitt **Sitzungen** von IGEL Setup (und gelegentlich auch in einigen anderen Abschnitten) sowie in der Funktion **Konfiguration bearbeiten** in der UMS verfügbar.

Um eine Sitzung zu kopieren, gehen Sie wie folgt vor:

1. Öffnen Sie im Setup den Menüpfad **Sitzungen > [Sitzungstyp] > [Sitzungstyp] Sitzungen**.
   Beispiel: **Sitzungen > RDP > RDP Sitzungen**
   Die vorhandenen Sitzungen werden angezeigt**.**
2. Markieren Sie die Sitzung, die Sie kopieren möchten.
3. Klicken Sie  .
   Eine Kopie der Sitzung wird im selben Ordner erstellt.

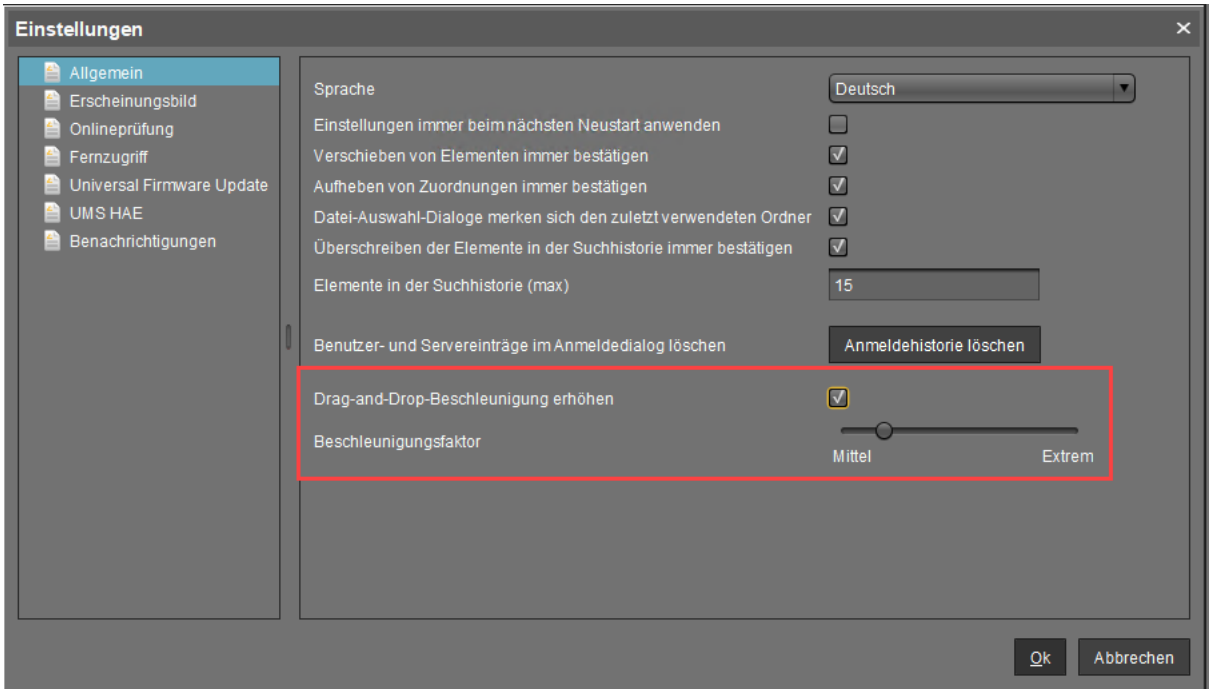
Drag & Drop-Beschleunigung für große Strukturbäume

Wenn Sie eine wirkliche große Anzahl an Objekten in Ihrer IGEL UMS (Universal Management Suite) haben, kann es mühsam sein, ein Objekt per Drag & Drop an eine neue Position zu ziehen, wenn die neue Position ganz weit von der aktuellen Position entfernt ist.

Aber mit UMS Version 5.03.100 oder neuer können Sie Ihre Scrollgeschwindigkeit erhöhen. Sobald das Objekt, das Sie bewegen, den unteren Rand des Strukturbaumfensters berührt, beginnt die Beschleunigung.

Um die Drag & Drop-Beschleunigung zu aktivieren:

1. Öffnen Sie die UMS und gehen Sie unter **Extras > Einstellungen > Allgemein**.
2. Aktivieren Sie **Drag-and-Drop-Beschleunigung erhöhen**.
3. Passen Sie den **Beschleunigungsfaktor** Ihren Bedürfnissen entsprechend an und klicken Sie auf **Ok**.



Drag & Drop-Beschleunigung ist bereit.

Mit der Smartcard lizenzieren schlägt fehl

Symptom

Sie können keine Lizenzen von Smartcard in die IGEL UMS **(License Management)** erstellen, obwohl gültige Lizenzen auf der SIM / Smartcard gespeichert sind und der Treiber des Smartcardlesers auf Ihrem System installiert ist.

- Der Smartcardleser zeigt ein Problem im Windows Hardware Manager **[!].**

Problem

Ein weiterer Smartcardleser (z. B. eingebauter Kartenleser) übersteuert den Zugriff.

Lösung

Deaktivieren oder deinstallieren sie alle anderen Smartcardleser im Windows Hardware Manager.

UMS Referenzhandbuch

Was ist neu - Aktualisierungen in der Knowledge Base für IGEL UMS 12.04.100

Auf dieser Seite finden Sie eine Zusammenfassung der aktualisierten Dokumentation mit direkten Links zu den akutalisierten Artikeln.

⚠ Aufgrund der bevorstehenden Migration der Knowledge Base wird der Inhalt von UMS 12.04.120 bereits einige Tage vor dem eigentlichen Release veröffentlicht.

ⓘ Die Release Notes zur IGEL Universal Management Suite 12 finden Sie sowohl als Textdatei im gleichen Ordner wie die Installationsprogramme auf unserem Download-Server[16].

⚠ Vor der Installation / dem Update der IGEL UMS lesen Sie bitte Einstieg in IGEL COSMOS.
Ohne die UMS Web App können Sie keine IGEL OS 12 Geräte verwalten. Daher muss die UMS Web App bei der Installation der UMS ausgewählt werden.

Reverse Proxy / Load Balancer Beispielkonfigurationen

Beispielhafte Netzwerkkonfigurationen mit der Verwendung von Reverse Proxies von Drittanbietern wurden aktualisiert. Für weitere Informationen siehe:

- IGEL Universal Management Suite Network Configuration (see page 17)
- Configure the UMS for Integrating Reverse Proxy with SSL Offloading (see page 18)
- NGINX: Example Configuration for as Reverse Proxy in IGEL OS with SSL Offloading (see page 19)
- F5 BIG IP: Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading (see page 20)
- Azure Application Gateway: Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading (see page 21)
- Citrix Netscaler: Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading (see page 22)

Migrieren von HA UMS zu Standalone UMS

Beschreibung hinzugefügt, um die Migration durchzuführen. Für weitere Informationen siehe How to Migrate an UMS High Availability Installation to a Standalone UMS (see page 160).

16 https://www.igel.com/software-downloads/cosmos/

Troubleshooting bei HA-Migration

Fehlersuche IPv6-Einstellung hinzugefügt. Für weitere Informationen siehe Troubleshooting: UMS 12 HA Not Working After Upgrade (see page 162).

UMS Web App

Automatische Cleanup von App-Versionen

Der UMS App Proxy bereinigt einmal pro Woche automatisch den lokalen Cache, um den belegten Speicherplatz klein zu halten. Dies kann unter **Apps > Einstellungen** aktiviert/deaktiviert werden. Für weitere Informationen siehe Configuring Global Settings for the Update of IGEL OS Apps (see page 889).

Sperren des Herunterladens aus dem IGEL App Portal

Es wurde ein Parameter hinzugefügt, mit dem Geräte daran gehindert werden, das öffentliche App-Portal als Download-Quelle zu verwenden. Dies kann unter **Apps > Einstellungen** aktiviert/deaktiviert werden. Für weitere Informationen siehe Configuring Global Settings for the Update of IGEL OS Apps (see page 889).

Unified App Import Button

Die Funktion zum Hochladen von Apps wurde vereinheitlicht und das Verhalten wurde verbessert. Für weitere Informationen siehe Export und Hochladen von Apps in der IGEL UMS (see page 894).

Überblick über die IGEL UMS

Mit der IGEL Universal Management Suite (UMS) können Sie IGEL OS Geräte per Fernzugriff konfigurieren und steuern. Eine Übersicht über die von der IGEL UMS unterstützten Geräte finden Sie unter Geräte, die von der IGEL Universal Management Suite (UMS) unterstützt werden (see page 5).

Die UMS unterstützt neben unterschiedlichen Betriebssystemen auch Datenbanken und Verzeichnisdienste wie Microsoft Active Directory.

Typische Einsatzgebiete der IGEL UMS

- Automatische Einrichtung von Geräten
- Konfiguration von Geräten, Software-Clients, Tools und lokalen Protokollen
- Verteilung von Updates
- Diagnose und Support

Eigenschaften der IGEL UMS

Schnelle Installation:

Ein Assistent hilft Ihnen bei der Installation. Alternativ zur integrierten Datenbank können Sie externe Datenbanksysteme anbinden.

Einfache Verwaltung per Mausklick:

Die meisten Hardware- bzw. Softwareeinstellungen können Sie mit wenigen Klicks ändern.

Einheitliche Benutzeroberfläche:

Die UMS Benutzeroberfläche gleicht der lokalen Gerätekonfiguration. Die zusätzlichen Remote Management-Funktionen ermöglichen dem Administrator volle Kontrolle in gewohnter und bewährter Umgebung.

Kein Scripting:

Obwohl Scripting unterstützt wird, wird es nur im absoluten Ausnahmefall für die Steuerung der Gerätekonfiguration benötigt.

Asset Management:

Automatische Erfassung sämtlicher Hardwareinformationen, lizenzierter Features und installierter Hotfixes.

Kommentarfelder:

Für verschiedene kundenspezifische Informationen wie Standort, Installationsdatum oder Inventarnummer.

Unterstützung zahlreicher Betriebssysteme:

Der UMS Server kann auf vielen gängigen Versionen von Microsoft Windows Server und Linux ausgeführt werden.

Betriebssystemunabhängiger Zugriff:

Die UMS Konsole läuft auf jedem Gerät, das mit dem Java Runtime Environment ausgestattet ist. Die UMS Web App kann in jedem unterstützten Browser geöffnet werden.

Verschlüsselte Kommunikation:

Zertifikatsbasierte, TLS/SSL-verschlüsselte Kommunikation zwischen Remote Management-Servern und Clients für den Schutz vor nicht berechtigter Neukonfiguration der Geräte.

Ausfallsichere Updatefunktion:

Wenn ein Gerät während des Update-Prozesses ausfällt, z. B. durch Stromausfall oder Verlust der Netzwerkverbindung, bleibt das Gerät funktionsfähig. Der Update-Vorgang wird beim nächsten Start abgeschlossen.

Basiert auf Standard-Kommunikationsprotokollen:

Eine Neukonfiguration der Router und Firewalls ist nicht erforderlich, da UMS die Standard-Protokolle HTTP und FTP nutzt.

Unterstützung umfassender Umgebungen:

Die IGEL Universal Management Suite ist auf mehrere tausend Geräte skalierbar.

Gruppen- und profilbasierte Verwaltung:

Geräte innerhalb einer Organisationseinheit können einfach über Profile verwaltet werden. Wechseln Mitarbeiter in eine andere Abteilung, kann der Administrator die neuen Einstellungen problemlos per Drag-and-Drop vornehmen.

Problemloser Roll-out:

Wenn Sie Vorgabeverzeichnisregeln konfigurieren, können IGEL OS Geräte automatisch in ein gewünschtes Verzeichnis, z. B. auf Basis des jeweiligen Subnetzes, platziert werden. Die Geräte erhalten dann automatisch die Konfigurationseinstellungen, die Sie für dieses Verzeichnis definiert haben.

Umfassende Unterstützung aller Konfigurationsparameter:

Die Steuerung der meisten IGEL Geräteeinstellungen wie z. B. die Geräte- oder Sitzungskonfiguration erfolgt mithilfe der UMS Benutzeroberfläche.

Übertragung von administrativen Rechten:

Große Organisationen können mehrere Systemadministratoren für jeweils unterschiedliche Steuerungs- und Berechtigungsbereiche bevollmächtigen. Diese administrativen Konten können aus einem Active Directory importiert werden.

Planung von Aufgaben:

Wartungsaufgaben können für die Nachtstunden eingeplant werden, sodass der tägliche Betrieb nicht beeinträchtigt wird.

VNC Shadowing:

Das IT-Support-Team kann remote auf die Bildschirme der Geräte zugreifen, um Probleme zügig zu identifizieren und dem Benutzer die Lösung direkt zu demonstrieren.

Komponenten der IGEL UMS

Die IGEL Universal Management Suite (UMS) besteht aus folgenden Komponenten:

- UMS Server

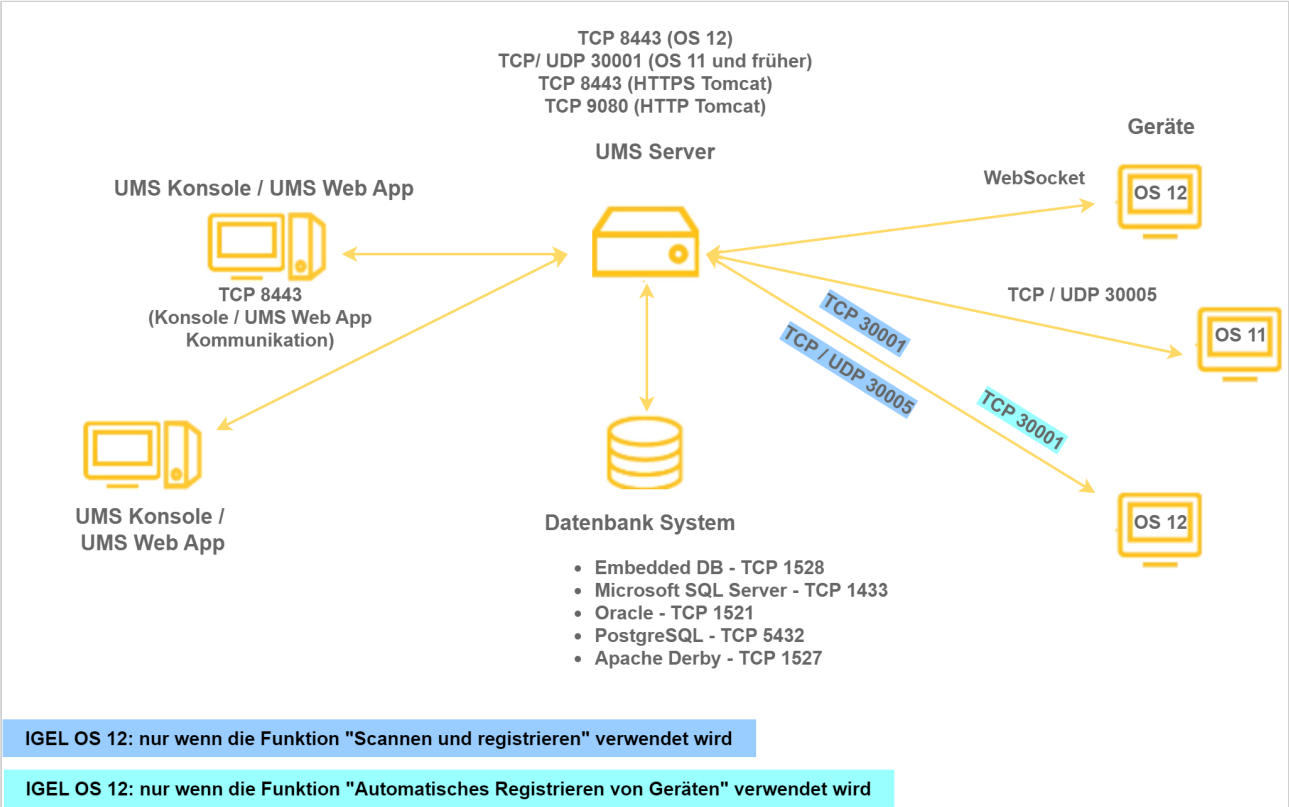
- UMS Administrator
- UMS Konsole / UMS Web App

UMS Server

Der UMS Server ist eine Serveranwendung, für die ein Datenbankmanagement-System (RDBMS) erforderlich ist. Die Datenbank kann sowohl auf dem Server selbst als auch auf einem Remote Host installiert sein. Detaillierte Informationen zur unterstützten Umgebung finden Sie in den Release Notes (see page 965). Siehe auch Installationsvoraussetzungen für die IGEL UMS (see page 250).

Typischerweise sind die UMS Konsole und der UMS Server auf verschiedenen Rechnern installiert.

Der UMS Server kommuniziert intern mit der Datenbank und extern mit den registrierten Geräten sowie mit der UMS Konsole / UMS Web App:



Die Datenübertragung zwischen UMS Server und Geräten sowie zwischen UMS Server und UMS Konsole / UMS Web App ist verschlüsselt.

Für die Kommunikation mit IGEL OS 11-Geräten gibt es zwei Protokolle, die auf separaten Kommunikationsports (30001 und 30005) laufen - eines für die Kommunikation der Geräte mit der UMS und ein anderes für die Kommunikation der UMS mit dem Gerät. Mit der Einführung der IGEL Cloud Services wurde auch das Unified Protocol eingeführt. Das Unified Protocol wird für die gesamte Kommunikation zwischen der UMS und den OS 12-Geräten verwendet. Dieser einzige Kommunikationspfad wird über eine WebSocket-Verbindung realisiert, was eine dauerhafte, bidirektionale Vollduplex-TCP-Verbindung zwischen UMS 12 und OS 12-Geräten ermöglicht. Die Verwendung einer WebSocket-Verbindung ermöglicht es, den Netzwerkverkehr durch die Komprimierung von Befehlen zu reduzieren, die Sicherheit durch die Verwendung von Clientzertifikaten und Sicherheitstokens für das

Onboarding von Geräten zu erhöhen und einen neuen Device Connector-Service auf der UMS und den IGEL Cloud Gateways einzuführen, der Ihre IGEL Umgebung auf zukünftige Cloud-Funktionen vorbereitet. Mehr Informationen zu Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).

Alle Konfigurationen der verwalteten Geräte sind in der Datenbank gespeichert. Änderungen einer Konfiguration werden in der Datenbank durchgeführt und bei Bedarf an das Gerät übertragen. Das Gerät kann die Informationen beim Startvorgang aus der Datenbank abrufen oder Sie können die neue Konfiguration manuell an das Gerät senden. Ein zeitgesteuertes Update der Konfiguration ist ebenfalls möglich.

UMS Administrator

Der UMS Administrator ist eine Verwaltungskomponente des UMS Servers.

Zentrale Bestandteile des UMS Administrators sind:

- Netzwerkkonfiguration (Ports)
- Datenbankkonfiguration (Datenquellen, Backups)

Weitere Informationen zum UMS Administrator finden Sie unter Der IGEL UMS Administrator (see page 707).

UMS Konsole / UMS Web App

Die Verwaltung der IGEL OS Geräte und deren Konfiguration erfolgt über die GUI der UMS Konsole und der UMS Web App.

Zentrale Aufgaben der UMS Konsole und der UMS Web App sind:

- Darstellung der Konfigurationsparameter der Geräte
- Einrichtung von Profilen und geplanten Aufgaben
- Verwaltung von IGEL OS Updates

UMS Konsole

Die UMS Konsole ist die Java-basierte Benutzerschnittstelle zum UMS Server. Detaillierte Informationen zur UMS Konsole finden Sie unter Benutzeroberfläche der UMS Konsole (see page 340).

Wie Sie sich bei der UMS Konsole anmelden können, erfahren Sie unter UMS Konsole mit dem IGEL UMS Server verbinden (see page 319).

UMS Web App

Die UMS Web App ist die webbasierte Benutzerschnittstelle zum UMS Server. Detaillierte Informationen zur Anwendung finden Sie unter IGEL UMS Web App (see page 783). Wie Sie sich mit der UMS Web App verbinden, erfahren Sie unter Wie kann ich mich an der IGEL UMS Web App anmelden? (see page 786)

> ⚠ Die UMS Web App kann derzeit nur zusätzlich zur UMS Konsole verwendet werden. Einige Funktionen sind momentan nur in der UMS Web App verfügbar (z. B. Erstellung von Profilen für IGEL OS 12 Geräte, Verwaltung von IGEL OS Apps), andere - nur in der UMS Konsole (z. B. geplante Aufgaben, Benutzerberechtigungen und Zugriffskontrolle). Für die feature matrix, siehe Feature Matrix: UMS Web App vs. UMS Console (see page 242).

Feature Matrix: UMS Web App vs. UMS Console

Dieser Artikel beschreibt die in der IGEL Universal Management Suite (UMS) Console und in der IGEL UMS Web App verfügbaren Funktionen.

- Die UMS Web App kann derzeit nur zusätzlich zur Java-basierten UMS Konsole verwendet werden.
- Der Funktionsumfang der UMS Web App wird ständig erweitert.
- Alle Features, die bereits in der UMS Web App verfügbar sind, werden vollständig unterstützt.

Feature-Matrix: UMS Web App vs. UMS Konsole

Konfigurationsdialog, Profile, Zuweisungen und Apps

		UMS Konsole	UMS Web App
Konfiguration bearbeiten	**OS 12 Geräte**	✓	✓
	OS 11 Geräte	✓	✓
Profile erstellen und bearbeiten	**OS 12 Geräte**	✗	✓
	OS 11 Geräte	✓	✓
Profile kopieren	**OS 12 Geräte**	✗	✗
	OS 11 Geräte	✓	✗
Profile löschen		✓	✗
Zuweisungen verwalten		✓	✓
IGEL OS Apps verwalten		✗	✓
Geräte als Profile exportieren	**OS 12 Geräte**	✗	✓
Geräte als Profile importieren (="Profile importieren" in der UMS Web App)	**OS 11 Geräte**	✓	✗

Profile exportieren/ importieren	**OS 12 Geräte**	✗	✓
	OS 11 Geräte	✓	✗
IGEL OS Apps exportieren/hochladen		✗	✓

Gerätebefehle

	UMS Konsole	UMS Web App
Spiegeln	✓	✓
Sicheres Terminal	✓	✗
Befehle für Energiesteuerung	✓	✓
Befehle für Synchronisation	✓	✓
Auf Werkseinstellungen zurücksetzen	✓	✓
Erweiterte Befehle	✓	✗

Die in der UMS Konsole verfügbaren Gerätebefehle finden Sie unter Menüleiste der IGEL UMS Konsole (see page 343).

Eine detaillierte Liste der Gerätebefehle, die in der UMS Web App verfügbar sind, finden Sie unter Geräte - Ihre Endgeräte in der IGEL UMS Web App ansehen und verwalten (see page 799).

Erweiterte Verwaltung

	UMS Konsole	UMS Web App
Geräte löschen	✓	✗
Nach Geräten scannen und Geräte registrieren	✓	✓
Views (="Suche" in der UMS Web App)	✓	✓
Jobs	✓	✗
Administrative Aufgaben	✓	✗
URL-Datei-Verwaltung	✓	✓
Papierkorb	✓	✗
Benutzerberechtigungen und Zugriffskontrolle	✓	✗
UMS Administration (UMS Netzwerk- & Globale Konfiguration-Einstellungen verwalten)	✓	✗

Logs und Supportinformationen

	UMS Konsole	UMS Web App
Protokolle der UMS Web App anzeigen	✗	✓
Protokolle der UMS Konsole anzeigen	✓	✓ (teilweise)
Protokollierung aktivieren	✓	✓
Protokolle löschen	✓	✓
Supportinformationen speichern	✓	✗
Gerätedateien für den Support speichern	✓	✗

Suche

	UMS Konsole	UMS Web App
Suche nach Geräten	✓	✓
Suche nach Views	✓	✗
Suche nach Profilen	✓	✗
Suchergebnisse exportieren	✓	✓

UMS Installieren und Aktualisieren

In diesem Kapitel finden Sie Informationen zu den folgenden Themen:

- Grundlagen der IGEL Universal Management Suite (UMS) Installationstypen und deren Anwendungsfälle: IGEL UMS Installation (see page 246)
- Software- und Hardwareanforderungen für die Installation von UMS-Komponenten: Installationsvoraussetzungen für die IGEL UMS (see page 250)
- Richtlinien und Empfehlungen zum Einrichten Ihrer UMS Umgebung: Leitlinien zur Installation und Größenbestimmung der IGEL UMS (see page 279)

Sie finden ausführliche Anleitungen zu den folgenden Aufgaben:

- Installation der Standard UMS mit eingebetteter Datenbank: IGEL UMS unter Linux installieren (see page 253) und IGEL UMS unter Windows installieren (see page 266)
- Distributed IGEL UMS installieren (see page 275)
- UMS aktualisieren (see page 298)
- Anbindung externer Datenbanksysteme (see page 308)

> Weitere Informationen zu spezifischen Themen finden Sie in den Artikeln unter UMS Installation (see page 67) und UMS Umgebung (see page 90).

IGEL UMS Installation

Dieser Artikel beschreibt mögliche Installationsoptionen für die IGEL Universal Management Suite (UMS) und gibt allgemeine Installationsempfehlungen und -anweisungen. Weitere Empfehlungen zur UMS Umgebung finden Sie unter Leitlinien zur Installation und Größenbestimmung der IGEL UMS (see page 279).

Eine UMS Installation kann aus einer einzelnen UMS Server-Instanz oder aus mehreren UMS Servern bestehen.

Bei einer Einzelinstanz-Installation (auch "**Standard UMS**" genannt) führt nur ein UMS Server alle Aufgaben aus und ist die einzige Zugangsstelle für die Endgeräte.

Bei einer Multiinstanz-Installation gibt es mehrere UMS Server, und jeder kann alle Aufgaben ausführen, aber einige Aufgaben sind zwischen den UMS Servern verteilt. Die Endgeräte können sich mit einem beliebigen UMS Server verbinden und sind nicht an diesen gebunden. Installationen mit mehreren Instanzen erfordern Messaging zwischen den Komponenten, um organisatorische Aufgaben zu unterstützen. Die IGEL UMS unterstützt zwei Arten von Multiinstanz-Installationen:

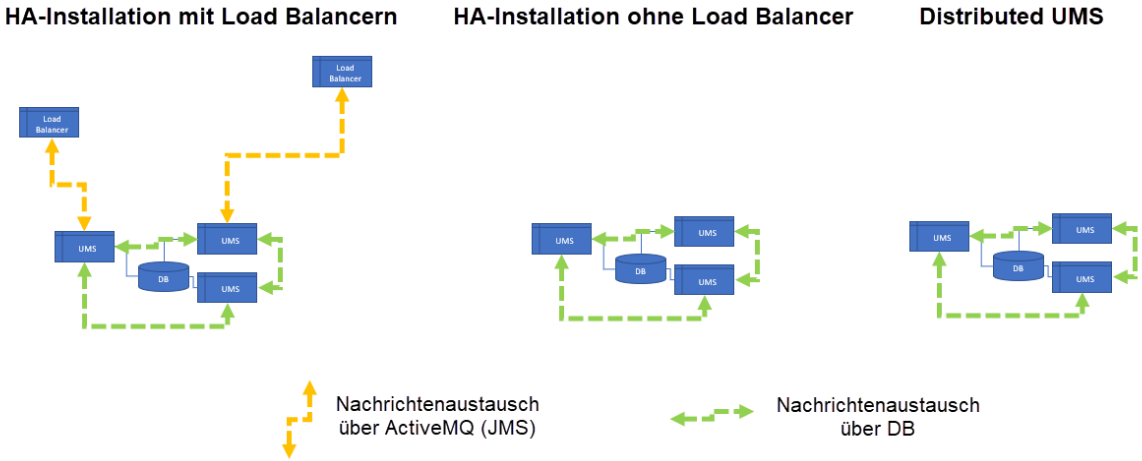
- **Distributed UMS**
  Bei einer Distributed UMS Installation werden alle UMS Server als Standalone-Server installiert, aber mit der aktivierten Distributed UMS-Funktion funktionieren diese UMS Server so, als ob sie als High Availability-Umgebung installiert wären. Nachrichten zwischen den UMS Servern verwenden eine Datenbankbrücke: Damit stehen alle Kernfunktionen von verteilten Aufgaben zur Verfügung.

  Eine Distributed UMS Installation hat folgende Voraussetzungen:
  - Gemeinsame externe Datenbank
  - 8443/TCP für den WebDav-Dateiaustausch

  Besonderheiten: Subnetzübergreifende Kommunikation und Installation in Cloud-Umgebungen wie Azure / AWS sind möglich. Zur Lastverteilung sollte eine DNS-Round-Robin-Lastverteilung der IP-Adresse des Servers verwendet werden, da IGEL UMS Load Balancer nicht unterstützt werden. Der DNS-Round-Robin für `igelrmserver` sollte auf alle Server zeigen.

> Alternativ kann ab UMS 12 ein Reverse Proxy / externer Load Balancer zur Lastverteilung eingesetzt werden; der FQDN und Port des externen Load Balancers / Reverse Proxys muss als Cluster-Adresse angegeben werden, siehe Server-Netzwerkeinstellungen in der IGEL UMS (see page 581).
> Beachten Sie das Folgende:
> - Die Cluster-Adresse dient nur zur Kommunikation über den Webserver-Port (see page 709) (Standard: 8443).
> - SSL kann auf dem Reverse Proxy / externen Load Balancer (siehe NGINX: Example Configuration for as Reverse Proxy in IGEL OS with SSL Offloading (see page 19)) oder auf dem UMS Server terminiert werden.

- **UMS High Availability (HA) Erweiterung**
  Die UMS HA (see page 909) bietet alle Funktionen der Distributed UMS, jedoch mit der Möglichkeit, UMS Load Balancer zu installieren. Die Kommunikation zwischen den Komponenten der UMS HA-Installation, d. h. UMS Servern und UMS Load Balancern, ist durch die Verwendung desselben IGEL Netzwerktokens möglich.
  Ab UMS Version 6.10 verwenden Nachrichten zwischen den UMS Servern die Datenbankbrücke, nicht ActiveMQ wie bei früheren UMS Versionen. Dies gilt für alle HA-Installationen, unabhängig davon, ob UMS Load Balancer verwendet werden oder nicht. ActiveMQ-Messaging bleibt dabei weiterhin aktiv: bei HA-Installationen ohne Load Balancer ist es nur im Hintergrund aktiv; bei HA-Installationen mit UMS Load Balancern wird ActiveMQ-Messaging weiterhin für den Nachrichtenaustausch mit den Load Balancern verwendet, was die subnetzübergreifende Kommunikation und die Installation der UMS HA mit Load Balancern in Cloud-Umgebungen unmöglich macht. Weitere Informationen zum Messaging finden Sie unter UMS HA Statusprüfung - Ihre High Availability- und Distributed UMS-Systeme analysieren (see page 944).
  Mehr zum Austausch von Nachrichten...



  Eine UMS HA-Installation hat folgende Voraussetzungen:
  - Gemeinsame externe Datenbank
  - 8443/TCP für den WebDav-Dateiaustausch
  - Für HA-Installationen mit IGEL UMS Load Balancern: 6155/UDP, 61616/TCP ActiveMQ Messaging. Die Liste der UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).

Besonderheiten der HA-Installationen mit IGEL UMS Load Balancern: Alle UMS Server und UMS Load Balancer müssen sich im selben VLAN befinden; es gibt keine Unterstützung für Cloud-Umgebungen wie Azure / AWS.

Subnetzübergreifende Kommunikation für UMS HA-Installationen ohne UMS Load Balancer
Bestehende UMS HA-Installationen ohne UMS Load Balancer können weiterhin verwendet werden - eine Neuinstallation als Distributed UMS ist nicht erforderlich. Die subnetzübergreifende Kommunikation von UMS Servern wird mit dem Update auf UMS 6.10 oder höher automatisch möglich.

Eine Neuinstallation ist auch deshalb nicht notwendig, weil eine UMS HA ohne Load Balancer im Wesentlichen wie die Distributed UMS funktioniert - beide sind identisch in Bezug auf die Synchronisierung von Dateien (see page 151), Firmware, Zertifikaten, Lizenzen und Jobs; beide nutzen die Datenbankbrücke für den Nachrichtenaustausch.

Zwischen UMS Standardinstallation, Distributed UMS und UMS High Availability wählen

Allgemeine Installationsempfehlungen
Für kleine Installationen ist in der Regel eine einzelne UMS Server-Instanz ("Standard UMS") mit einer eingebetteten Datenbank ausreichend. Bei Bedarf kann eine Einzelinstanz-Installation jederzeit durch die Installation zusätzlicher Server zu einer Distributed UMS-Installation erweitert werden (im Falle einer eingebetteten Datenbank ist der Umstieg auf eine externe Datenquelle nötig).
Große Installationen sollen entweder die UMS High Availability oder die Distributed UMS (bevorzugt bei Neuinstallationen, da z. B. keine zusätzlichen Firewallausnahmen konfiguriert werden müssen) verwenden. Für große Installationen wird auch der Einsatz von DNS-Round-Robin-Lastverteilung oder IGEL Cloud Gateway empfohlen.
Siehe auch Leitlinien zur Installation und Größenbestimmung der IGEL UMS (see page 279)

- Sie sind ein **Bestandskunde** und haben eine UMS Einzelinstanz-Installation, möchten aber zusätzliche UMS Server betreiben...
  => Installieren Sie UMS 12.01 oder höher ("Standard UMS" im UMS Installer) auf dem ersten Server und aktivieren Sie die Distributed UMS-Funktion. Danach können Sie weitere Server (als Distributed UMS) installieren und mit der gleichen Datenbank (NICHT Embedded-DB) verbinden.
- Sie sind ein **Bestandskunde** und haben die UMS High Availability installiert...
  => Installieren Sie UMS 12.01 oder höher ("UMS High Availability Network"-Komponenten im UMS Installer; siehe Installation eines HA-Netzwerks aktualisieren (see page 931)) und belassen Sie alles, wie es ist.
- Sie sind ein **Neukunde** und möchten eine UMS Einzelinstanz-Installation...
  => Installieren Sie "Standard UMS" 12.01 oder höher.
- Sie sind ein **Neukunde** und möchten die UMS mit mehreren Servern betreiben, benötigen aber keine IGEL UMS Load Balancer, da Sie DNS-Round-Robin-Lastverteilung einsetzen...
  => Installieren Sie UMS 12.01 oder höher ("Distributed UMS" im UMS Installer) auf dem ersten Server. Danach können Sie die anderen Server auch als Distributed UMS installieren und mit der gleichen Datenbank (NICHT Embedded-DB) verbinden.
- Sie sind ein **Neukunde** und möchten die UMS mit mehreren Servern betreiben und die IGEL UMS Load Balancer nutzen...
  => Installieren Sie UMS 12.01 oder höher als High Availability mit Load Balancern. Fragen Sie aber vorher bei IGEL nach, ob es nicht besser wäre, auf den Einsatz von IGEL UMS Load Balancern zu verzichten, weil diese für große Installationen möglicherweise nicht optimal sind. Verwenden Sie auch IGEL Cloud Gateway für die Verwaltung von Geräten außerhalb des Unternehmensnetzwerks.
- Sie sind ein **Neukunde** und möchten die UMS mit mehreren Servern in der Cloud betreiben...
  => Installieren Sie UMS 12.01 oder höher ("Distributed UMS" im UMS Installer) auf dem ersten Server. Danach können Sie die anderen Server auch als Distributed UMS installieren und mit der gleichen Datenbank (NICHT Embedded-DB) verbinden.

IGEL UMS installieren

- Für die Verwaltung der UMS-Installation benötigen Sie die UMS Konsole. Bei Multiinstanz-Installationen muss die UMS Konsole nicht unbedingt auf jedem UMS Server installiert sein.
  Hinweis: Aus Sicherheits-, Leistungs- oder anderen Gründen wird die UMS Konsole häufig zusätzlich auf einem separaten Host installiert.
- Ohne die UMS Web App können Sie keine IGEL OS 12-Geräte verwalten. Daher muss die UMS Web App bei der Installation der UMS ausgewählt werden. Bei Multiinstanz-Installationen muss die UMS Web App nicht unbedingt auf jedem UMS Server installiert sein, siehe Wichtige Informationen zur IGEL UMS Web App (see page 784).
- Bei der Installation des UMS Servers wird automatisch die Anwendung UMS Administrator installiert, die für die Verwaltung der UMS-Installation erforderlich ist.

Informationen zu den Komponenten der UMS finden Sie unter Überblick über die IGEL UMS (see page 238).

Standard UMS

Wenn Sie sich für eine UMS Einzelinstanz-Installation entschieden haben, lesen Sie die folgenden Artikel. Sie beschreiben das vollständige Verfahren zur Standardinstallation der UMS mit eingebetteter Datenbank. Wenn Ihre gewünschte Installation davon abweicht, können Sie einzelne Komponenten auswählen, z. B. für eine einzelne Konsoleninstallation.

- IGEL UMS unter Linux installieren (see page 253)
- IGEL UMS unter Windows installieren (see page 266)

Distributed UMS

Wenn Sie die Distributed UMS installieren oder Ihre bestehende UMS Standardinstallation auf die Distributed UMS erweitern möchten, siehe Distributed IGEL UMS installieren (see page 275).

UMS High Availability

Wenn Sie die UMS High-Availability-Erweiterung (see page 909) installieren möchten, siehe HA-Installation (see page 914).

Installationsvoraussetzungen für die IGEL UMS

In diesem Artikel werden die Mindestanforderungen an Ihre Hardware und Software aufgeführt, die für eine erfolgreiche Installation der Komponenten der IGEL Universal Management Suite (UMS) Umgebung erfüllt sein müssen. Einzelheiten zu den IGEL UMS-Komponenten finden Sie unter Überblick über die IGEL UMS (see page 238).

Systemanforderungen

Sie können die IGEL UMS auf Windows und Linux (x86_64) betreiben.

> Angaben zu den unterstützten Betriebssystemen finden Sie im Abschnitt "Supported Environment" der Release Notes (see page 965).

Voraussetzungen der Standard UMS

UMS Server und UMS Administrator

Bei der Einzelinstanz-Installation (auch Standard UMS genannt) muss Ihre Hardware und Software die folgenden Mindestanforderungen erfüllen, um den **UMS Server** und den **UMS Administrator** zu hosten:

- Mind. 5 GB RAM
- Mind. 22 GB freier Speicherplatz
- 4 CPUs

> Unter Linux ist ein X11-System erforderlich. Es wird von der Anwendung UMS Administrator benötigt, die sich nur auf derselben Maschine wie der UMS Server starten lässt.

- Installieren Sie den UMS Server nicht auf einem Domänencontroller-System.
- Die manuelle Änderung des Java Runtime Environment auf dem UMS Server wird nicht empfohlen.
- Der Betrieb zusätzlicher Apache Tomcat-Webserver zusammen mit dem UMS Server wird nicht empfohlen.

Voraussetzungen der UMS Komponenten

Sie können sich dafür entscheiden, andere UMS-Komponenten auf demselben Host zu installieren wie den UMS Server und den UMS Administrator. In diesem Fall haben die Komponenten die folgenden Mindestanforderungen:

- **UMS Web App**
  - Mind. 1 GB RAM
- **UMS Konsole**

    - Mind. 3 GB RAM
    - Mind. 1 GB freier Speicherplatz

- **Embedded-Datenbank**
    - Mind. 2 GB freier Speicherplatz

Standard UMS mit UMS Konsole und Embedded-Datenbank

Wenn sowohl die UMS Konsole als auch die Embedded-Datenbank einbezogen werden, erhöhen sich die Anforderungen an RAM und Speicherplatz wie folgt:

- Mind. 8 GB RAM
  (5 GB für UMS Server und UMS Administrator + 3 GB für UMS Konsole)
- Mind. 25 GB freier Speicherplatz
  (22 GB für UMS Server und UMS Administrator + 1 GB für UMS Konsole + 2 GB für Embedded DB)
- 4 CPUs

Standard UMS mit UMS Konsole, Embedded-Datenbank und UMS Web App

Wenn sowohl die UMS Konsole als auch die Embedded-Datenbank und die UMS Web App einbezogen werden, erhöhen sich die Anforderungen an RAM und Speicherplatz wie folgt:

- Mind. 9 GB RAM
  (5 GB für UMS Server und UMS Administrator + 3 GB für UMS Konsole + 1 GB für UMS Web App)
- Mind. 25 GB freier Speicherplatz
  (22 GB für UMS Server und UMS Administrator + 1 GB für UMS Konsole + 2 GB für Embedded DB)
- 4 CPUs

Voraussetzungen für die Installation einer alleinstehenden UMS Konsole (standalone)

Um eine die UMS Konsole auf einem separaten Rechner zu installieren, muss Ihre Hardware die folgenden Mindestanforderungen erfüllen:

- Mind. 3 GB RAM
- Mind. 1 GB freier Speicherplatz
- 2 CPUs

Datenbanksysteme (DBMS)

> Angaben zu den unterstützten Datenbanksystemen finden Sie in den Release Notes (see page 965) im Bereich "Supported Environment". Die Installations- und Betriebsvoraussetzungen für die Datenbank finden Sie in der Dokumentation des jeweiligen DBMS.

High Availability

Die Installationsanforderungen für High Availability (see page 909) finden Sie unter HA: Installationsvoraussetzungen (see page 915).

Die Embedded-Datenbank kann nicht für ein HA-Netzwerk verwendet werden. Sie können die Embedded-Datenbank für eine reine Testinstallation mit nur einem einzigen Server für UMS Server und Load Balancer verwenden.

- High Availability mit IGEL UMS Load Balancern: Alle UMS Server und UMS Load Balancer müssen sich im **selben VLAN** befinden.
- Für High Availability (UMS HA) mit IGEL UMS Load Balancern muss der Netzwerkverkehr über den UDP-Broadcast-Port 6155 und der TCP-Verkehr sowie UDP-Broadcast-Verkehr über Port 61616 zugelassen werden. Weitere Informationen zu den UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).
- In der Netzwerkkonfiguration auf Windows-Servern muss die Option TCP/IPv6 für UMS 12 aktiviert sein.
- IGEL UMS HA Installation mit IGEL UMS Load Balancern wird in Cloud-Umgebungen wie Azure / AWS nicht unterstützt, da sie keinen Broadcast-Verkehr innerhalb ihrer Netzwerke zulassen. Die HA-Installation ohne IGEL UMS Load Balancer (sowie die Distributed UMS (see page 246)) wird jedoch in Cloud-Umgebungen ab UMS Version 6.10 unterstützt.

IGEL UMS unter Linux installieren

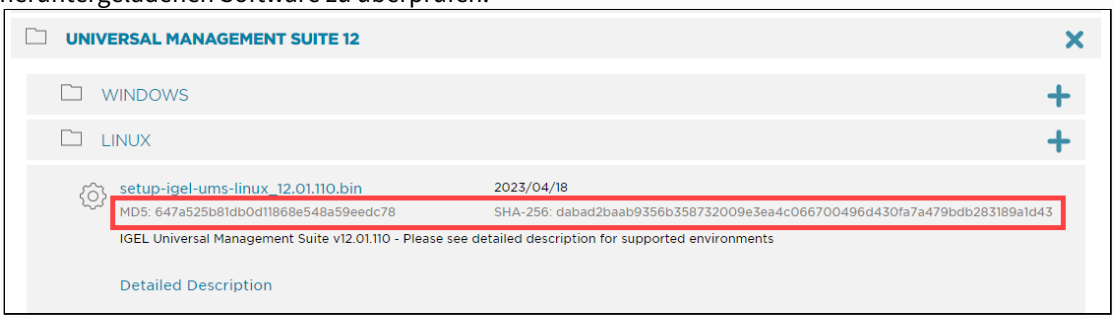
Dieser Artikel beschreibt das vollständige Verfahren zur Standardinstallation der IGEL Universal Management Suite (UMS) mit eingebetteter Datenbank unter Linux. Bei abweichenden Installationen wählen Sie die Komponenten einzeln aus, z. B. für eine einzelne Konsoleninstallation. Die Installationsvoraussetzungen können Sie unter Installationsvoraussetzungen für die IGEL UMS überprüfen.

> Angaben zu den unterstützten Betriebssystemen finden Sie im Abschnitt "Supported Environment" der Release Notes (see page 965).

So installieren Sie die IGEL Universal Management Suite unter Linux:

1. Laden Sie die aktuelle Version der IGEL Universal Management Suite vom IGEL Downloadserver[17] herunter.

   > Aus Integritäts- und Sicherheitsgründen empfiehlt es sich, die Prüfsumme (Checksum) der heruntergeladenen Software zu überprüfen.

2. Öffnen Sie einen Terminalemulator wie beispielsweise xterm und wechseln Sie in das Verzeichnis, in dem sich die Installationsdatei `setup-igel-ums-linux-[Version].bin` befindet.

3. Überprüfen Sie, ob die Datei ausführbar ist. Falls nicht, lässt sie sich mit folgendem Befehl ausführbar machen:
   `chmod u+x setup*.bin`

   > Sie brauchen `root/sudo`-Rechte, um die Installation durchzuführen.

17 https://www.igel.com/software-downloads/

4. Führen Sie die Installationsdatei als `root` oder mit `sudo` aus:
   `sudo ./setup-igel-ums-linux-[Version].bin`
   Dies entpackt die Dateien ins Verzeichnis `/tmp`, startet die enthaltene Java Virtual Machine und entfernt die temporären Dateien nach dem Installationsvorgang.

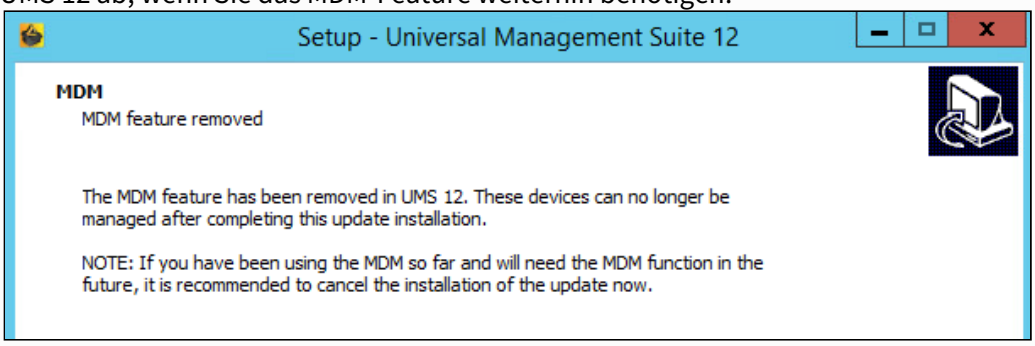
5. Starten Sie den Installationsvorgang mit **Enter**.

   > Sie können die Installation jederzeit durch zweimaliges Drücken der Taste [Esc] abbrechen.

6. Lesen und bestätigen Sie die Lizenzvereinbarung.

7. Wählen Sie unter **Destination directory** das Verzeichnis, in das die UMS installiert werden soll. (Standard: `/opt/IGEL/RemoteManager`)

8. Wenn Sie eine existierende UMS Installation aktualisieren: Wählen Sie unter **Database backup** eine Datei für das Backup der Embedded-Datenbank sowie von Lizenzen und Zertifikaten. Falls Sie bereits ein Backup erstellt haben, können Sie auch **No (continue)** wählen, um diesen Schritt zu überspringen. Siehe auch IGEL UMS unter Linux aktualisieren (see page 300).

   > **Nur für Update-Installationen**
   > - Ab UMS 12 ist das MDM-Feature nicht mehr verfügbar. Brechen Sie das Upgrade auf UMS 12 ab, wenn Sie das MDM-Feature weiterhin benötigen:
   >
   > 
   >
   >
   > - Nur wenn Sie eine Distributed UMS-Installation haben: Während der Update-Installation wird geprüft, ob nur ein UMS Server läuft und die anderen gestoppt sind. Wenn dies nicht der Fall ist, stoppen Sie alle UMS Server bis auf einen und fahren Sie mit der Aktualisierung fort; andernfalls riskieren Sie einen Datenverlust. Nachdem die Aktualisierung auf diesem Server abgeschlossen ist, können Sie die übrigen UMS Server aktualisieren, entweder parallel oder nacheinander.

9. Wählen Sie unter **Installation type** den Installationsumfang:
   - **Complete**: UMS Server und UMS Konsole
   - **Distributed UMS**: Distributed UMS Installation (see page 246)
   - **HA Net**: High-Availability (see page 909)-Konfiguration
   - **Client only**: nur UMS Konsole

10. Wählen Sie, ob die IGEL UMS Web App (see page 783) installiert werden soll. Siehe Wichtige Informationen zur IGEL UMS Web App (see page 784).

11. Bestätigen Sie unter **system requirements**, dass Ihr System die angezeigten Systemanforderungen erfüllt.

12. Bestätigen oder geben Sie die IP-Adresse des UMS Servers unter **Confirm server IP address** ein. Diese IP-Adresse wird für die Erstellung des UMS Server-Zertifikats beim ersten Start verwendet. Dieser Dialog wird nur bei der ersten Installation einer UMS Version angezeigt, die dieses Feature beinhaltet.

    ⚠ Wenn Sie bei der Installation der UMS die IP-Adresse nicht anpassen, enthält das Webzertifikat Ihres UMS Servers die falsche IP-Adresse, was zu Problemen bei der Geräteregistrierung usw. führt. Um das Problem zu lösen, muss ein neues Webzertifikat erstellt werden. Siehe Ungültiges Webzertifikat und Fehler bei der Geräteregistrierung nach der Installation der IGEL UMS 12 unter Linux (see page 74).

13. Wählen Sie unter **Data directory** das Verzeichnis, in dem Universal Firmware Updates und Dateien gespeichert werden sollen. (Standard: `/opt/IGEL/RemoteManager`)

    ❗ Dateien und Firmwareupdates werden im Verzeichnis `ums_filetransfer` gespeichert. Frei wählbare Verzeichnisse für Dateiübertragungen werden nicht unterstützt.

14. Wählen Sie unter **Database** das gewünschte Datenbanksystem.
    - **Internal**: Die Embedded-Datenbank
    - **Other**: Ein externer Datenbankserver

    ⓘ Die Embedded-Datenbank eignet sich für die meisten Einsatzzwecke. Sie ist in der Standardinstallation enthalten.
    Die Verwendung eines externen Datenbanksystems wird in den folgenden Fällen empfohlen:
    - Sie möchten ein großes Netzwerk von Geräten verwalten.
    - In Ihrem Unternehmen ist bereits ein dediziertes Datenbanksystem im Einsatz.
    - Sie verwenden die High Availability- oder Distributed UMS Lösung.

    Weitere Informationen zur Verwendung der UMS mit externen Datenbanken finden Sie unter Anbindung externer Datenbanksysteme (see page 308).

15. Geben Sie **Benutzername** und **Passwort** für den Datenbankzugriff ein.
Die Anmeldedaten für die Verbindung mit der Datenbank werden erzeugt.

> Bei der Eingabe des Benutzernamens und des Passworts wird zwischen Groß- und Kleinschreibung unterschieden.
> Initial sind die hier eingegebenen Anmeldedaten zugleich die Anmeldedaten für den UMS Superuser. Nach der Installation können die Anmeldedaten für den Datenbankbenutzer und die für den UMS Superuser unabhängig voneinander geändert werden. Weitere Informationen finden Sie unter UMS Superuser ändern (see page 737).

16. Wählen Sie, ob Sie im Menü **Verknüpfungen** für UMS Konsole und UMS Administrator anlegen möchten.

17. Prüfen Sie die Zusammenfassung der Installationseinstellungen und starten Sie den Vorgang mit **Start installation**.
Falls Sie die Standardinstallation gewählt haben, wird der UMS Server samt Embedded-Datenbank installiert und gestartet.

18. Wenn der Installationsvorgang zu Ende ist, öffnen Sie die UMS Konsole über das Menü oder mit dem Befehl `/opt/IGEL/RemoteManager/RemoteManager.sh`

> Es wird allgemein NICHT empfohlen, den Befehl `RemoteManager.sh` als `sudo` auszuführen. Unter Red Hat Enterprise Linux 8 kann `RemoteManager.sh` nur ohne `sudo` ausgeführt werden.

19. Verbinden Sie die UMS Konsole mit dem UMS Server, indem Sie die Anmeldedaten für die Datenbank eingeben, die Sie bei der Installation festgelegt haben. Weitere Informationen finden Sie unter UMS Konsole mit dem IGEL UMS Server verbinden (see page 319).
Wie Sie eine Verbindung mit der UMS Web App herstellen, finden Sie unter Wie kann ich mich an der IGEL UMS Web App anmelden? (see page 786)

> Es wird empfohlen, Ihre Antivirensoftware und, falls installiert, andere Verwaltungssoftware wie HP Device Manager auf mögliche Konflikte zu überprüfen, wenn
> - die Installation der IGEL UMS fehlschlägt
> - der UMS Serverdienst nicht startet, wenn die Installation abgeschlossen ist, und der manuelle Start des Dienstes fehlschlägt. Einzelheiten zum Starten von Diensten finden Sie unter IGEL UMS HA-Dienste und -Prozesse (see page 949).
> - Probleme bei der Verbindung der UMS Konsole mit dem UMS Server auftreten

> **UMS 12 Kommunikationsports**

Wenn Sie Änderungen am Netzwerk vornehmen möchten, sollten Sie die folgenden Ports und Pfade berücksichtigen:

- Für IGEL OS 12-Geräte ist TCP 8443 /device-connector/* erforderlich.
  SSL kann am Reverse Proxy / externen Load Balancer (siehe IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading) oder am UMS Server terminiert werden.
- Für den Import von IGEL OS 12 Apps vom IGEL App Portal in die UMS ist die URL https://app.igel.com/ (TCP 443) erforderlich.
- Für die UMS Web App sind TCP 8443 /webapp/* und /wums-app/* erforderlich.
- Für die UMS Konsole ist der Root erforderlich, d. h. TCP 8443 /*
- Für IGEL OS 11-Geräte sind TCP 30001 und TCP/UDP 30005 erforderlich.

Weitere Informationen zu UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).

Falls Sie einen externen Load Balancer / Reverse Proxy verwenden
Der FQDN und Port Ihres externen Load Balancers / Reverse Proxy muss in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Server-Netzwerkeinstellungen > Cluster-Adresse** angegeben werden. Informationen zur Cluster-Adresse finden Sie unter Server-Netzwerkeinstellungen in der IGEL UMS (see page 581).

Um IGEL OS 12-Geräte zu verwalten, müssen Sie Ihre UMS nach der Installation registrieren, siehe IGEL UMS registrieren (see page 321).

TechChannel

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=p52CxtB_0ok

- Amazon Linux 2 für die UMS Installation vorbereiten (see page 258)
- UMS auf Red Hat Enterprise Linux (RHEL) 8 installieren (see page 259)
- UMS auf Red Hat Enterprise Linux (RHEL) 7.3 installieren (see page 261)
- UMS auf Oracle Linux Server installieren (see page 263)
- Installing IGEL UMS on Microsoft Azure (see page 265)

Amazon Linux 2 für die UMS Installation vorbereiten

Überblick

Sie können die UMS auf Amazon Linux 2 installieren, sowohl in der Cloud als auch auf einem eigenen Rechner.

Wenn Sie die UMS Konsole oder den UMS Aministrator unter Amazon Linux 2 verwenden wollen, müssen Sie die Desktopumgebung Mate installieren und einrichten.

Umgebung

Diese Beschreibung ist für die folgende Umgebung gültig:

- UMS 6.05 oder höher
- Amazon Linux 2, Cloud oder auf eigenem Rechner

Anleitung

1. Melden Sie sich unter Amazon Linux 2 als Benutzer mit `sudo` -Berechtigung an.
2. Aktualisieren Sie alle Paketquellen:
   `sudo yum update`
3. Installieren Sie die Desktopumgebung Mate:
   `sudo amazon-linux-extras install mate-desktop1.x`
4. Gehen Sie zu `/etc/sysconfig/` und erstellen Sie mit einem Texteditor eine Datei mit dem Namen `desktop`
5. Geben Sie in die Datei `desktop` den folgenden Inhalt ein:
   `PREFERRED=/usr/bin/mate-session`
6. Speichern Sie die Datei.
7. Gehen Sie in Ihr Homeverzeichnis und erstellen Sie eine Datei mit dem Namen `.Xclients`
8. Geben Sie den folgenden Inhalt in die Datei `.Xclients` ein:
   `/usr/bin/mate-session`
9. Speichern Sie die Datei.
10. Machen Sie die Datei `.Xclients` ausführbar:
    `chmod +x ~/.Xclients`
    Sie können nun die UMS installieren, siehe die Anleitung IGEL UMS unter Linux installieren (see page 253).

UMS auf Red Hat Enterprise Linux (RHEL) 8 installieren

Sie möchten die UMS auf der 64-Bit-Version von Red Hat Enterprise Linux (RHEL) 8 installieren.

> Die Installation der UMS auf RHEL 8 kann auf einem reinen RHEL 8-System (Server mit GUI) erfolgen.

Vor der Installation von UMS (oder UMS HA, siehe HA-Installation (see page 914)) sind die folgenden Schritte durchzuführen:

1. Aktualisieren Sie als `root` die lokale Paketdatenbank und starten Sie den Server neu.

   ```
   # yum -y update
   ```

   Die UMS Installation wird zusätzliche Module herunterladen, wenn diese noch nicht installiert sind: `qt5-qtbase`

2. Setzen Sie die `TERM` -Variable wie folgt, insbesondere wenn auf dem Server eine graphische Benutzeroberfläche (GUI) installiert ist.

   ```
   # export TERM=xterm
   ```

3. Machen Sie das Verzeichnis `/root` beschreibbar.

   Standardmäßig hat das Verzeichnis `/root` kein Schreiben-Flag gesetzt. Da die Standardinstallation von UMS HA das Netzwerkkonfigurationsarchiv in diesem Verzeichnis erstellt, muss dieses Verzeichnis das Schreiben-Flag für den `root` -Benutzer erhalten.

   ```
   # sudo chmod u+w /root
   ```

4. Konfigurieren Sie die Firewall.
   RHEL 8 wird mit einer aktivierten Firewall geliefert. Damit UMS und UMS HA ordnungsgemäß funktionieren, müssen die folgenden Ports im aktiven Profil geöffnet werden (z. B. IGEL UMS Kommunikationsports (see page 6)):

   ```
   # 8443/tcp 9080/tcp 30001/tcp 30002 tcp 61616/tcp 61616/udp 1528/tcp 6155/udp
   ```

   Um diese Ports zu öffnen, müssen die folgenden Befehle ausgeführt werden:

   ```
   # sudo firewall-cmd --zone=public --add-port=8443/tcp --permanent
   # sudo firewall-cmd --zone=public --add-port=9080/tcp --permanent
   # sudo firewall-cmd --zone=public --add-port=30001/tcp --permanent
   ```

```
# sudo firewall-cmd --zone=public --add-port=30002/tcp --permanent
# sudo firewall-cmd --zone=public --add-port= 61616/tcp --permanent
# sudo firewall-cmd --zone=public --add-port= 61616/udp --permanent
# sudo firewall-cmd --zone=public --add-port= 1528/tcp --permanent
# sudo firewall-cmd --zone=public --add-port= 6155/udp --permanent
```

5. Fahren Sie mit der Installation der UMS fort, wie es in IGEL UMS unter Linux installieren (see page 253) beschrieben ist.

UMS auf Red Hat Enterprise Linux (RHEL) 7.3 installieren

Sie möchten die UMS auf der 64-Bit-Version von Red Hat Enterprise Linux (RHEL) 7.3 installieren.

Ab UMS 5.09

Ab UMS Version 5.09 wird die Installation der 32-Bit-Bibliotheken nicht mehr benötigt. Die notwendigen Abhängigkeiten werden automatisch installiert, wenn bei der UMS Installation die entsprechende Option gewählt wurde.

1. Passen Sie die Firewall-Einstellungen vom RHEL-Server an, um die von der UMS verwendeten Netzwerkports zuzulassen, siehe IGEL UMS Communication Ports (see page 6).
2. Schließen Sie die Installation ab, wie es in IGEL UMS unter Linux installieren (see page 253) beschrieben ist.

Ab UMS 5.07.100

Ab UMS Version 5.07.100 werden die benötigten 32-Bit-Bibliotheken automatisch vom UMS Installer installiert, falls die entsprechende Option während der Installation der UMS gewählt wurde.

1. Passen Sie die Firewall-Einstellungen vom RHEL-Server an, um die von der UMS verwendeten Netzwerkports zuzulassen, siehe IGEL UMS Kommunikationsports (see page 6).
2. Schließen Sie die Installation ab, wie es in IGEL UMS unter Linux installieren (see page 253) beschrieben ist.

Vor UMS 5.07.100

Um die UMS auf der 64-Bit-Version von RHEL 7.3 zu installieren:

1. Aktualisieren Sie als `root` Ihre 64-Bit-Pakete auf die neueste Version:
   ```
   yum update
   ```
2. Installieren Sie Bibliotheken für die 32-Bit-Unterstützung:
   ```
   yum install \
   glibc.i686 \
   libzip.i686 \
   ncurses-libs.i686 \
   bzip2-libs.i686 \
   libXtst.i686 \
   libXinerama.i686 \
   libXi.i686 \
   libXext.i686 \
   libXrender.i686 \
   libgcc.i686
   ```

3. Starten Sie neu.
4. Passen Sie die Firewall-Einstellungen vom RHEL-Server an, um die von der UMS verwendeten Netzwerkports zuzulassen, siehe IGEL UMS Kommunikationsports (see page 6).
5. Schließen Sie die Installation ab, wie es in IGEL UMS unter Linux installieren (see page 253) beschrieben ist.

Es gibt einen Fehler auf Red Hat Enterprise Linux (RHEL) 7.3 mit GNOME Desktop Version 3.14, wenn die UMS Konsole ausgeführt wird. Das Hauptfenster der UMS Konsole wird als leeres graues Rechteck angezeigt, da die GUI nicht korrekt dargestellt wird. Als Workaround kann die Größe des Fensters durch Ziehen der Fensterkanten oder durch Doppelklicken am oberen Rand (Maximieren) an der Stelle, an der sich die Titelleiste befinden würde, geändert werden. Dies löst einen Neuaufbau aus und das Fenster der UMS Konsole wird dann korrekt angezeigt.
Alternativ können Sie auch die KDE-Desktop-Umgebung auf RHEL 7.3 verwenden.

UMS auf Oracle Linux Server installieren

Oracle

Für den ordnungsgemäßen Betrieb der UMS mit Oracle-Datenbanken, insbesondere für den Aktualisierungsvorgang, muss die Anzahl von `open_cursors` für die Datenbank angepasst werden. `open_cursors` ist eine Systemeinstellung.

1. Um den aktuellen Wert zu erfahren, melden Sie sich als `SYSDBA` an der Datenbank an und führen Sie aus:
   `SQL> select name, value from v$parameter where name = 'open_cursors';`
2. Der empfohlene Wert für `open_cursors` ist "3000". Um den Wert zu setzen, führen Sie den folgenden Befehl als `SYSDBA` aus:
   `SQL> alter system set open_cursors = 3000 scope=both;`
3. Der gleiche Befehl sollte der `SPFILE` des Oracle-Systems hinzugefügt werden, damit die Änderungen beim nächsten Neustart erhalten bleiben.

Sie möchten die UMS auf der 64-Bit-Version von Oracle Linux Server installieren.

Ab UMS 5.09

Ab UMS Version 5.09 wird die Installation der 32-Bit-Bibliotheken nicht mehr benötigt. Die notwendigen Abhängigkeiten werden automatisch installiert, wenn bei der UMS Installation die entsprechende Option gewählt wurde. Informationen zur UMS Installation finden Sie unter IGEL UMS unter Linux installieren (see page 253).

1. Passen Sie die Firewall-Einstellungen vom Oracle Linux Server an, um die von der UMS verwendeten Netzwerkports zuzulassen, siehe IGEL UMS Kommunikationsports (see page 6).
2. Schließen Sie die Installation ab, wie es in IGEL UMS unter Linux installieren (see page 253) beschrieben ist.

Ab UMS 5.07.100

Ab UMS Version 5.07.100 werden die benötigten 32-Bit-Bibliotheken automatisch vom UMS Installer installiert, falls die entsprechende Option während der Installation der UMS gewählt wurde.

1. Passen Sie die Firewall-Einstellungen vom Oracle Linux Server an, um die von der UMS verwendeten Netzwerkports zuzulassen, siehe IGEL UMS Kommunikationsports (see page 6).
2. Schließen Sie die Installation ab, wie es in IGEL UMS unter Linux installieren (see page 253) beschrieben ist.

Vor UMS 5.07.100

Um die UMS auf der 64-Bit-Version von Oracle Linux Server zu installieren:

1. Aktualisieren Sie als `root` Ihre 64-Bit-Pakete auf die neueste Version:
   ```
   yum update
   ```
2. Installieren Sie Bibliotheken für die 32-Bit-Unterstützung:
   ```
   yum install \
   glibc.i686 \
   libzip.i686 \
   ncurses-libs.i686 \
   bzip2-libs.i686 \
   libXtst.i686 \
   libXinerama.i686 \
   libXi.i686 \
   libXext.i686 \
   libXrender.i686 \
   libgcc.i686
   ```
3. Starten Sie neu.
4. Passen Sie die Firewall-Einstellungen von Oracle Linux Server an, um die von der UMS verwendeten Netzwerkports zuzulassen, siehe IGEL UMS Kommunikationsports (see page 6).
5. Schließen Sie die Installation ab, wie es in IGEL UMS unter Linux installieren (see page 253) beschrieben ist.

Installing IGEL UMS on Microsoft Azure

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

IGEL UMS unter Windows installieren

Dieser Artikel beschreibt das vollständige Verfahren zur Standardinstallation der IGEL Universal Management Suite (UMS) mit eingebetteter Datenbank unter Windows. Bei abweichenden Installationen wählen Sie die Komponenten einzeln aus, z. B. für eine einzelne Konsoleninstallation. Die Installationsvoraussetzungen können Sie unter Installationsvoraussetzungen für die IGEL UMS (see page 250) überprüfen.

> Angaben zu den unterstützten Betriebssystemen finden Sie im Abschnitt "Supported Environment" der Release Notes (see page 965).

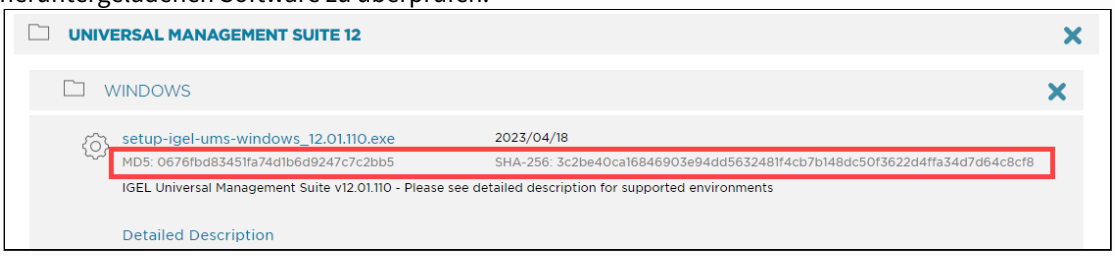
> Die Server Core-Installationsoption in Microsoft Windows Server wird nicht unterstützt.

Standardinstallation der UMS

So installieren Sie die IGEL UMS unter Windows:

1. Laden Sie die aktuelle Version der IGEL Universal Management Suite vom IGEL Downloadserver[18] herunter.

   > Aus Integritäts- und Sicherheitsgründen empfiehlt es sich, die Prüfsumme (Checksum) der heruntergeladenen Software zu überprüfen.

2. Starten Sie den Installer.

   > Sie benötigen Administratorrechte, um die UMS installieren zu können.

3. Lesen und bestätigen Sie die Lizenzvereinbarung unter **License Agreement**.

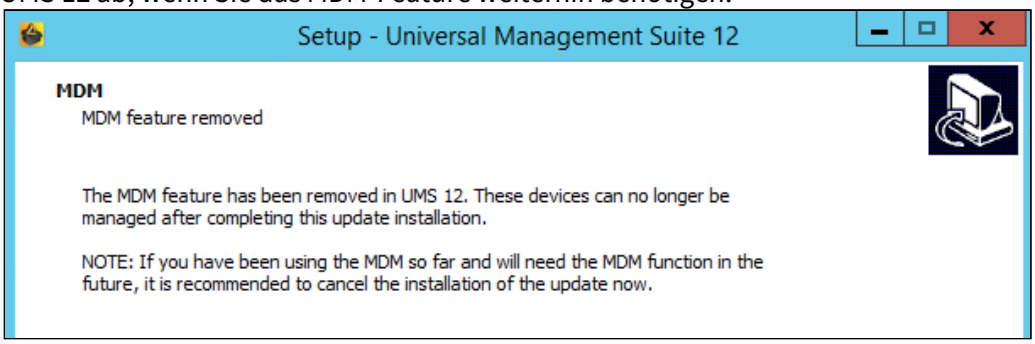
4. Lesen Sie die **Information** über den Installationsprozess und klicken Sie **Next**.

18 https://www.igel.com/software-downloads/

5. Nur wenn dies eine Update-Installation ist: Wählen Sie den Dateinamen für die Sicherung (**backup**) der Embedded-Datenbank. Wenn Sie keinen Dateinamen wählen und auf **Next** klicken, wird keine Sicherung erstellt. Siehe auch IGEL UMS unter Windows aktualisieren (see page 304).

   Nur für Update-Installationen

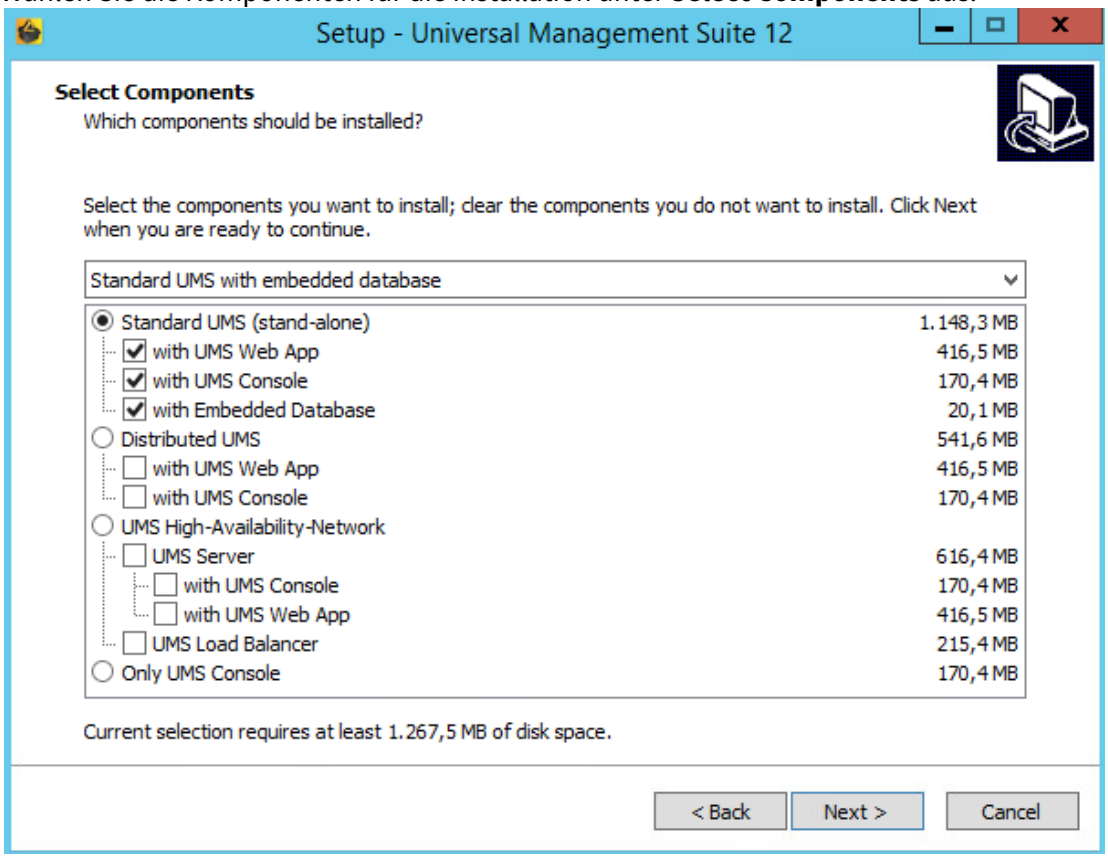
   - Ab UMS 12 ist das MDM-Feature nicht mehr verfügbar. Brechen Sie das Upgrade auf UMS 12 ab, wenn Sie das MDM-Feature weiterhin benötigen:

   - Nur wenn Sie eine Distributed UMS-Installation haben: Während der Update-Installation wird geprüft, ob nur ein UMS Server läuft und die anderen gestoppt sind. Wenn dies nicht der Fall ist, stoppen Sie alle UMS Server bis auf einen und fahren Sie mit der Aktualisierung fort; andernfalls riskieren Sie einen Datenverlust. Nachdem die Aktualisierung auf diesem Server abgeschlossen ist, können Sie die übrigen UMS Server aktualisieren, entweder parallel oder nacheinander.

6. Nur wenn dies eine Neuinstallation ist: Wählen Sie den Zielordner für die Installation unter **Select Destination Location**. (Standard: `C:\Programme\IGEL\RemoteManager`)

7. Wählen Sie die Komponenten für die Installation unter **Select Components** aus:



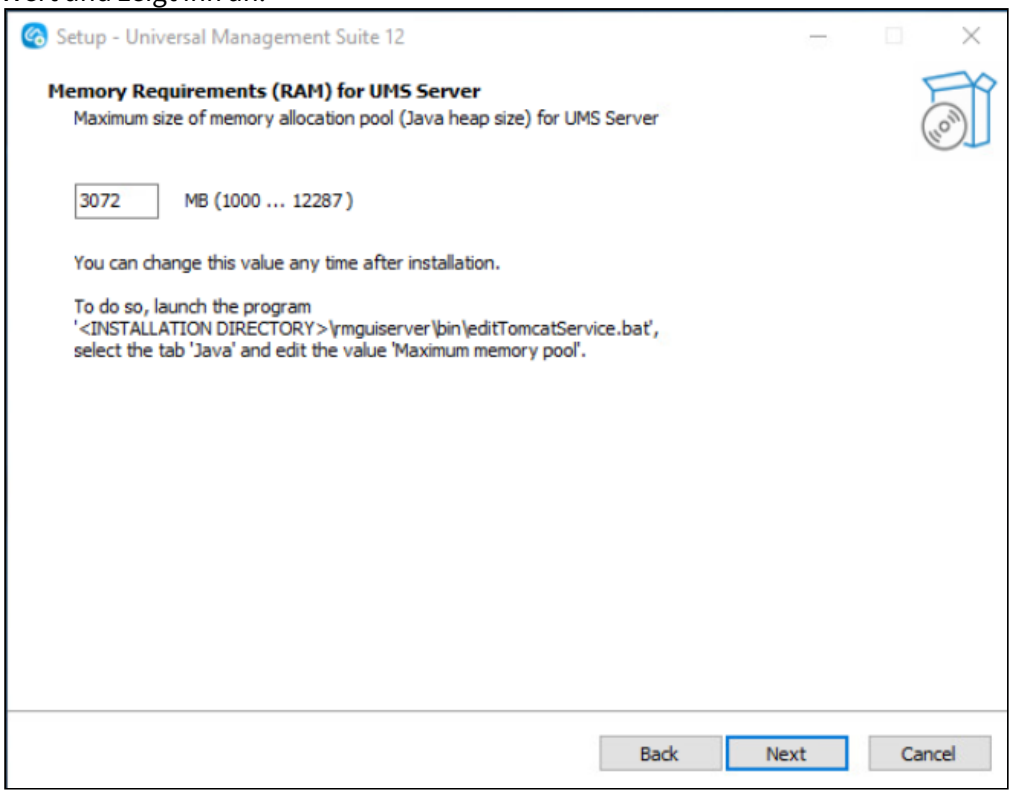
- **Standard UMS**
  - **with UMS Web App**
  - **with UMS Console**
  - **with Embedded Database**
- **Distributed UMS**
  - **with UMS Web App**
  - **with UMS Console**
- **UMS High Availability Network**
  - **UMS Server**
    - **with UMS Console**
    - **with UMS Web App**
  - **UMS Load Balancer**
- **Only UMS Console**

  Informationen zu den UMS-Installationstypen finden Sie unter IGEL UMS Installation (see page 246).

  Informationen zu den UMS-Komponenten finden Sie unter Überblick über die IGEL UMS (see page 238).

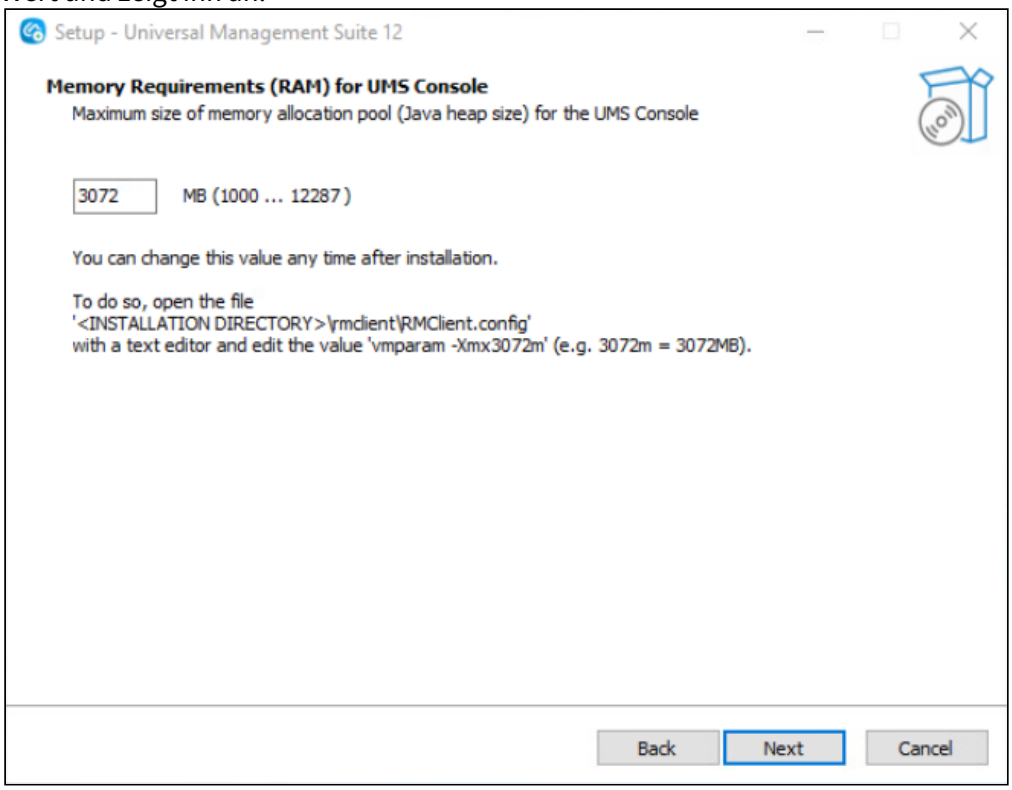
> Die Embedded-Datenbank eignet sich für die meisten Einsatzzwecke. Falls nicht deaktiviert, wird die Embedded-Datenbank automatisch installiert, wenn Sie **Standard UMS** auswählen.
> Die Verwendung eines externen Datenbanksystems wird in den folgenden Fällen empfohlen:
> - Sie möchten ein großes Netzwerk von Geräten verwalten.
> - In Ihrem Unternehmen ist bereits ein dediziertes Datenbanksystem im Einsatz.
> - Sie verwenden die High Availability- oder Distributed UMS-Lösung.
>
> Weitere Informationen zur Verwendung von UMS mit externen Datenbanken finden Sie unter Anbindung externer Datenbanksysteme (see page 308).

8. Legen Sie den maximalen Speicherbedarf (Java heap size) des UMS Server in Abhängigkeit von Ihrer Umgebung fest. Bei der Erstinstallation können Sie den Standardwert (3072 MB) beibehalten und ihn später anhand von Wie konfiguriere ich die Java-Heap-Größe für den UMS Server? (see page 141) ändern. Wenn Sie die UMS aktualisieren, übernimmt der Installer den zuvor konfigurierten Wert und zeigt ihn an.



9. Legen Sie den maximalen Speicherbedarf (Java heap size) der UMS Konsole in Abhängigkeit von Ihrer Umgebung fest. Bei der Erstinstallation können Sie den Standardwert (3072 MB) beibehalten und ihn später anhand von Wie konfiguriere ich die Java-Heap-Größe für die UMS Konsole? (see page 144) ändern. Wenn Sie die UMS aktualisieren, übernimmt der Installer den zuvor konfigurierten

Wert und zeigt ihn an.



10. Lesen Sie die RAM-Anforderungen unter **Memory (RAM) requirements** und klicken Sie auf **Next**, wenn Ihr System sie erfüllt.

11. Wählen Sie das UMS Datenverzeichnis unter **UMS data directory**. (Standard: `C:\Programme\IGEL\RemoteManager`)

12. Unter **User Credentials for DB-connect** geben Sie einen Benutzernamen und ein Passwort für die Datenbankverbindung ein, sofern Sie nicht planen, die UMS mit einem MS SQL Server über Active Directory zu verbinden. Weitere Informationen zur Verbindung über AD finden Sie unter Connecting the UMS to an SQL Server via Active Directory (see page 266).
Die Anmeldedaten für die Verbindung mit der Datenbank werden erzeugt.

    > Bei der Eingabe des Benutzernamens und des Passworts wird zwischen Groß- und Kleinschreibung unterschieden.
    > Initial sind die hier eingegebenen Anmeldedaten zugleich die Anmeldedaten für den UMS Superuser. Nach der Installation können die Anmeldedaten für den Datenbankbenutzer und die für den UMS Superuser unabhängig voneinander geändert werden. Weitere Informationen finden Sie unter Benutzer "UMS Administrator" ändern (see page 737).

13. Wenn die interne Windows Firewall auf dem Hostrechner aktiv ist: Überprüfen Sie die Einstellungen unter **Windows firewall settings** und ändern Sie diese, falls nötig. Jeder Port, der

hier aktiviert ist, wird in der Windows Firewall auf dem Hostrechner des UMS Servers als Regel definiert.

> **UMS 12 Kommunikationsports**
> Wenn Sie Änderungen am Netzwerk vornehmen möchten, sollten Sie die folgenden Ports und Pfade berücksichtigen:
> - Für IGEL OS 12-Geräte ist TCP 8443 /device-connector/* erforderlich.
>   SSL kann am Reverse Proxy / externen Load Balancer (siehe IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading) oder am UMS Server terminiert werden.
> - Für den Import von IGEL OS 12 Apps vom IGEL App Portal in die UMS ist die URL https://app.igel.com/ (TCP 443) erforderlich.
> - Für die UMS Web App sind TCP 8443 /webapp/* und /wums-app/* erforderlich.
> - Für die UMS Konsole ist der Root erforderlich, d. h. TCP 8443 /*
> - Für IGEL OS 11-Geräte sind TCP 30001 und TCP/UDP 30005 erforderlich.
>
> Weitere Informationen zu UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).

14. Bestimmen Sie einen Namen für den Startmenü-Ordner unter **Select Start Menu Folder**.

15. Wählen Sie unter **Select Additional Tasks**, ob Sie auf dem Desktop Verknüpfungen für UMS Konsole und UMS Administrator (see page 707) anlegen möchten.

16. Lesen Sie die Zusammenfassung und starten Sie den Installationsprozess.
    Der Installer installiert die UMS, erstellt Einträge im Windows-Softwareverzeichnis sowie im Startmenü und, falls ausgewählt, legt die Verknüpfungen für die UMS Konsole und UMS Administrator auf dem Desktop ab.

17. Nach Abschluss der Installation schließen Sie das Programm mit einem Klick auf **Finish**.
    Wenn Sie die Standardinstallation gewählt haben, läuft der UMS Server mit der Embedded-Datenbank.

18. Starten Sie die UMS Konsole.

19. Verbinden Sie die UMS Konsole mit dem UMS Server mithilfe der Zugangsdaten für die Datenbank, die Sie bei der Installation eingegeben haben. Weitere Informationen finden Sie unter UMS Konsole mit dem IGEL UMS Server verbinden (see page 319).

20. Starten Sie die UMS Web App. Siehe Wie kann ich mich an der IGEL UMS Web App anmelden? (see page 786).

> Es wird empfohlen, Ihre Antivirensoftware und, falls installiert, andere Verwaltungssoftware wie HP Device Manager auf mögliche Konflikte zu überprüfen, wenn
> - die Installation der IGEL UMS fehlschlägt
> - der UMS Server-Dienst nicht startet, wenn die Installation abgeschlossen ist, und der manuelle Start des Dienstes fehlschlägt. Einzelheiten zum Starten von Diensten finden Sie unter IGEL UMS HA-Dienste und -Prozesse (see page 949).

- Probleme bei der Verbindung der UMS Konsole mit dem UMS Server auftreten

Falls Sie einen externen Load Balancer / Reverse Proxy verwenden
Der FQDN und Port Ihres externen Load Balancers / Reverse Proxy muss in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Server-Netzwerkeinstellungen > Cluster-Adresse** angegeben werden. Informationen zur Cluster-Adresse finden Sie unter Server-Netzwerkeinstellungen in der IGEL UMS (see page 581).

Um IGEL OS 12-Geräte zu verwalten, müssen Sie Ihre UMS nach der Installation registrieren, siehe IGEL UMS registrieren (see page 321).

TechChannel

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=3YJnFiE7y5w

Unbeaufsichtigte Installation der UMS Konsole

Sie können die Installation unbeaufsichtigt ("silent") durchführen, indem Sie zunächst eine `.inf`-Datei erstellen und dann die Installation per Befehlszeile starten. Weitere Informationen finden Sie unter Unbeaufsichtigte Installation der UMS Konsole (see page 273).

Die unbeaufsichtigte Installation ist nur für die UMS Konsole möglich, nicht jedoch für UMS Server, UMS Administrator oder UMS Web App.

Unbeaufsichtigte Installation der UMS Konsole

Aus Leistungs-, Sicherheits- oder anderen Gründen, wie z. B. Größe Ihrer IGEL Universal Management Suite (UMS) Installation (see page 281), haben Sie sich entschieden, die UMS Konsole nicht auf dem UMS Server-Host, sondern auf einem separaten Rechner zu installieren. Sie möchten die Installation jedoch unbeaufsichtigt durchführen. In diesem Fall können Sie die folgenden Anweisungen für eine unbeaufsichtigte Installation der UMS Konsole verwenden. Sie sind auch anwendbar, wenn Sie nach einem Update des UMS Servers die UMS Konsole auf den Rechnern aktualisieren müssen.

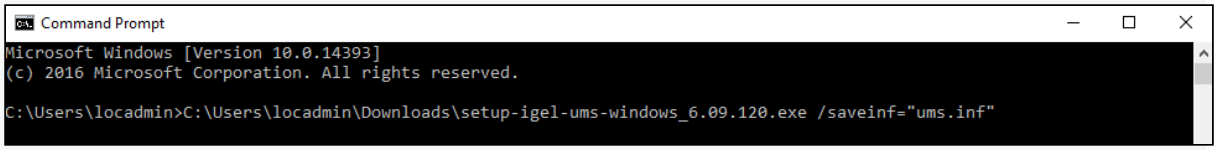
> Die unbeaufsichtigte Installation ist nur für die UMS Konsole möglich, nicht jedoch für UMS Administrator, UMS Server und UMS Web App.

> Diese Anweisungen gelten nur für den UMS Installer für Windows.

Führen Sie die folgenden Schritte für eine unbeaufsichtigte Installation der UMS Konsole durch:

1. Laden Sie die IGEL UMS vom IGEL Downloadserver[19] herunter. Wählen Sie die gleiche Version, die Sie für die Installation / Aktualisierung des UMS Servers verwendet haben.

2. Erstellen Sie in `cmd` oder `powershell` eine Konfigurationsdatei:
   `C:\[download directory]\setup-igel-ums-windows_x.y.z.exe /saveinf="[config-file]"`

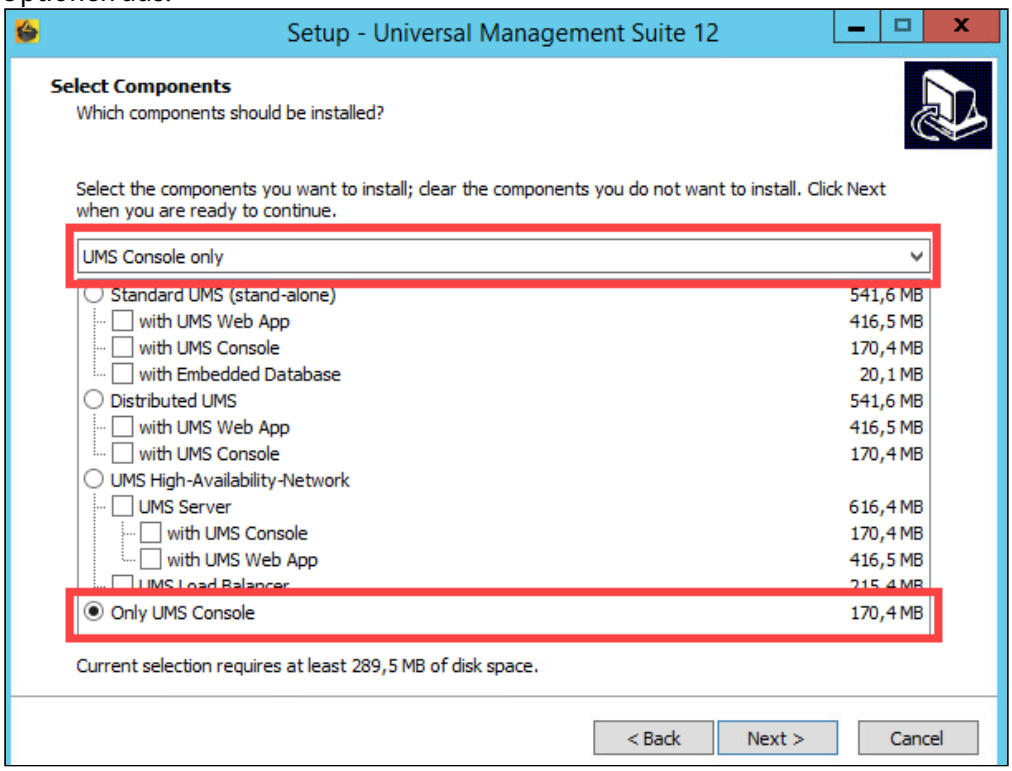
   

3. Bestätigen Sie den Dialog, dass Sie die Änderungen am Gerät vornehmen möchten.

4. Verwenden Sie den angezeigten Assistenten, um die Installation abzuschließen, während Sie sie in der Konfigurationsdatei aufnehmen. Wählen Sie dabei unter **Select Components** die folgenden

19 https://www.igel.com/software-downloads/

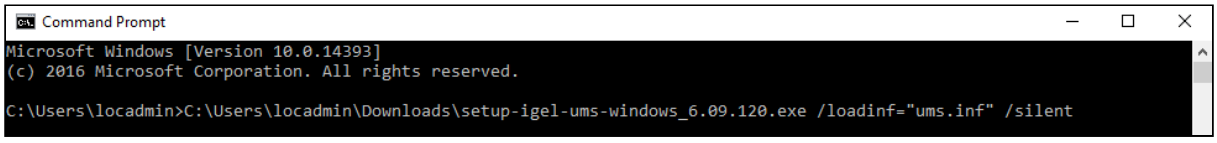
Optionen aus:



Wenn bereits andere UMS Komponenten auf dem Gerät installiert sind, ist die Option **Only UMS Console** deaktiviert und kann daher für die Installation nicht ausgewählt werden.

5. Übertragen Sie die UMS-Installationsdatei und die erstellte Konfigurationsdatei auf die Rechner, auf denen die UMS Konsole installiert / aktualisiert werden soll.

6. Verwenden Sie den folgenden Befehl, um die UMS Konsole zu installieren:
   `C:\[download-directory]\setup-igel-ums-windows_x.y.z.exe /loadinf="[config-file]" /silent`



Es kann ein Installationsfenster erscheinen, in dem der Benutzer aufgefordert wird, aber die Installation wird trotzdem im Hintergrund abgeschlossen.

Distributed IGEL UMS installieren

Dieser Artikel beschreibt die Installation der Distributed IGEL Universal Management Suite (UMS). Ausführliche Informationen zur Distributed UMS finden Sie unter IGEL UMS Installation (see page 246). Die folgenden Anweisungen können verwendet werden:

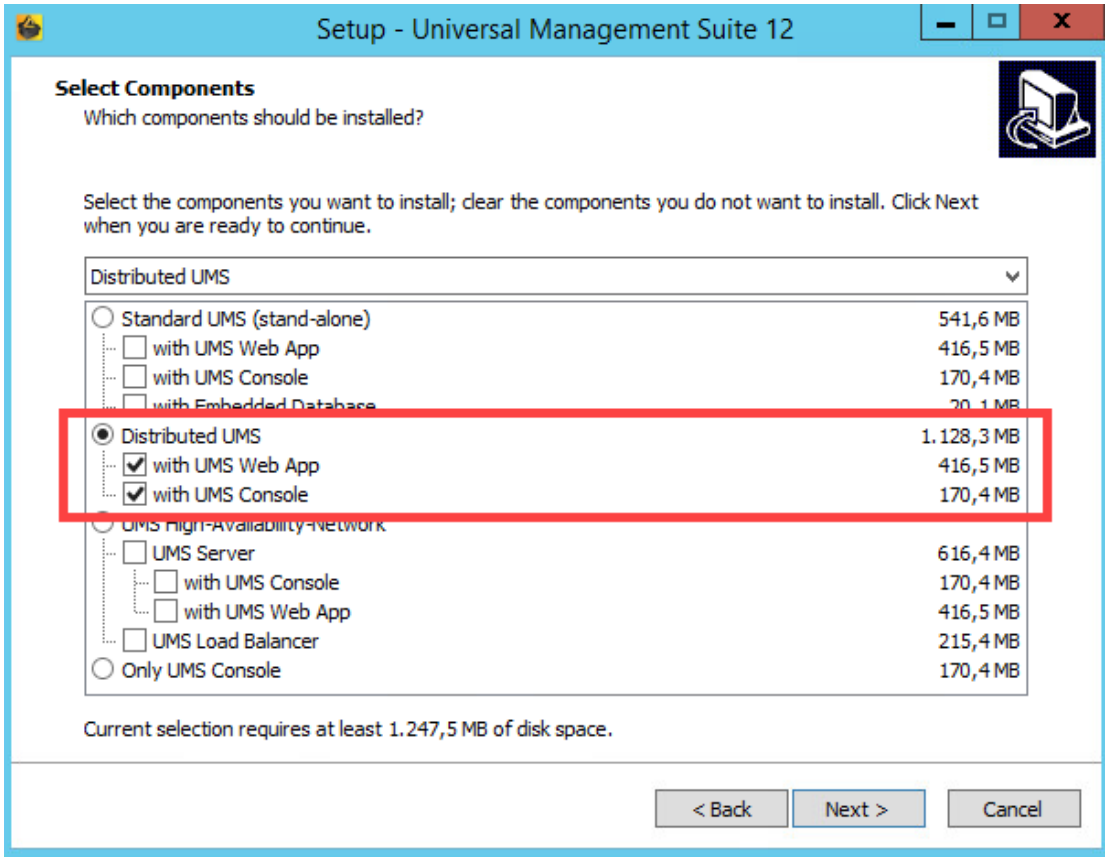
- wenn Sie eine Neuinstallation der Distributed UMS planen
- wenn Sie bereits eine UMS Standardinstallation haben, aber auf die Distributed UMS umsteigen wollen

> Zur Lastverteilung sollte eine DNS-Round-Robin-Lastverteilung der IP-Adresse des Servers verwendet werden. Der DNS-Round-Robin für `igelrmserver` sollte auf alle Server zeigen.

Neuinstallation der Distributed UMS

Um die Distributed UMS zu installieren, gehen Sie wie folgt vor:

1. Installieren Sie den ersten UMS Server. Die Anleitung dazu finden Sie unter IGEL UMS unter Windows installieren (see page 266) oder IGEL UMS unter Linux installieren (see page 253).
   Wählen Sie im UMS Installer **Distributed UMS**.



2. Konfigurieren Sie eine externe Datenbank, siehe Anbindung externer Datenbanksysteme (see page 308).

3. Fügen Sie diese Datenbank als Datenquelle im **UMS Administrator > Datenquelle > Neu** hinzu und **aktivieren** Sie diese. Siehe Wie kann ich eine Datenquelle im IGEL UMS Administrator einrichten? (see page 730)

4. Öffnen Sie die UMS Konsole und gehen Sie zu **UMS Administration > UMS Netzwerk > Server**, um zu prüfen, ob der Server läuft.

5. Installieren Sie weitere UMS Server (dabei aktivieren Sie **Distributed UMS** im UMS Installer) und verbinden Sie sie mit derselben Datenbank.

⚠ Wenn Sie die Distributed UMS-Funktion aktiviert haben und über mehrere UMS Server verfügen, seien Sie vorsichtig, falls Sie die Funktion deaktivieren möchten. Wenn die Distributed UMS-Funktion deaktiviert wird, aber mehrere UMS Server dieselbe Datenbank verwenden, wird keine Synchronisierung zwischen den UMS Servern durchgeführt.

Von einer UMS Standardinstallation auf eine Distributed UMS umsteigen

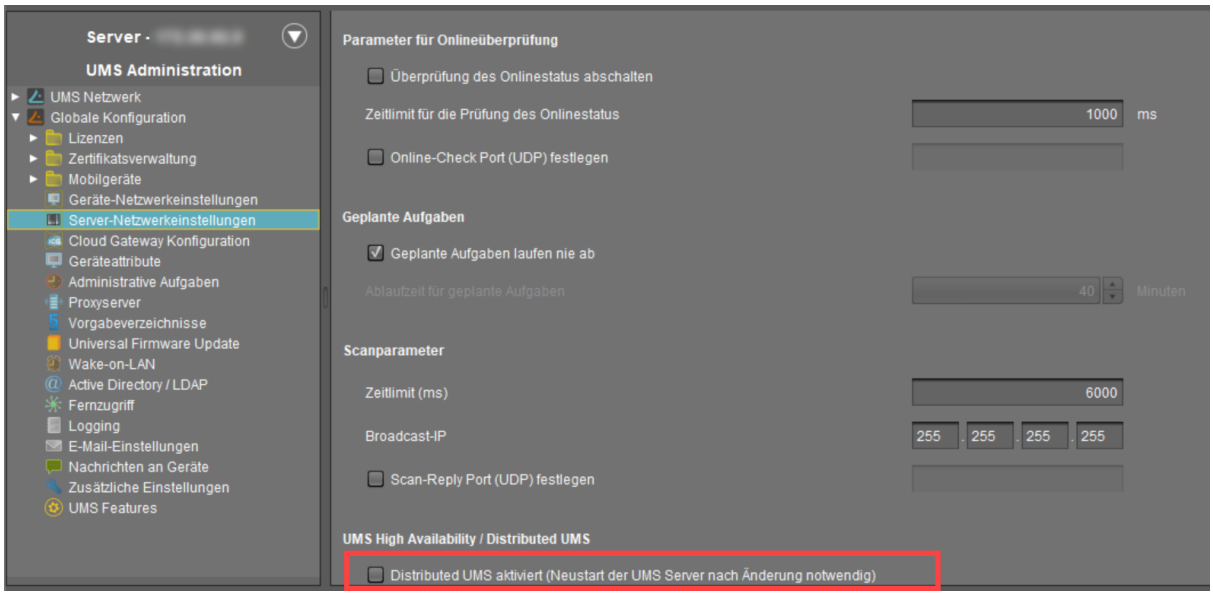
Wenn Sie Ihre bestehende UMS Standardinstallation auf die Distributed UMS erweitern möchten, gehen Sie wie folgt vor:

1. Wenn Sie eine UMS Standardinstallation mit einer externen Datenbank haben: Beginnen Sie mit Schritt 4.
   Wenn Sie eine UMS Standardinstallation mit einer eingebetteten Datenbank haben: Legen Sie eine neue externe Datenbank an (siehe Anbindung externer Datenbanksysteme (see page 308)) und fügen Sie diese Datenbank als Datenquelle im **UMS Administrator > Datenquelle > Neu** hinzu (siehe Wie kann ich eine Datenquelle im IGEL UMS Administrator einrichten? (see page 730)).

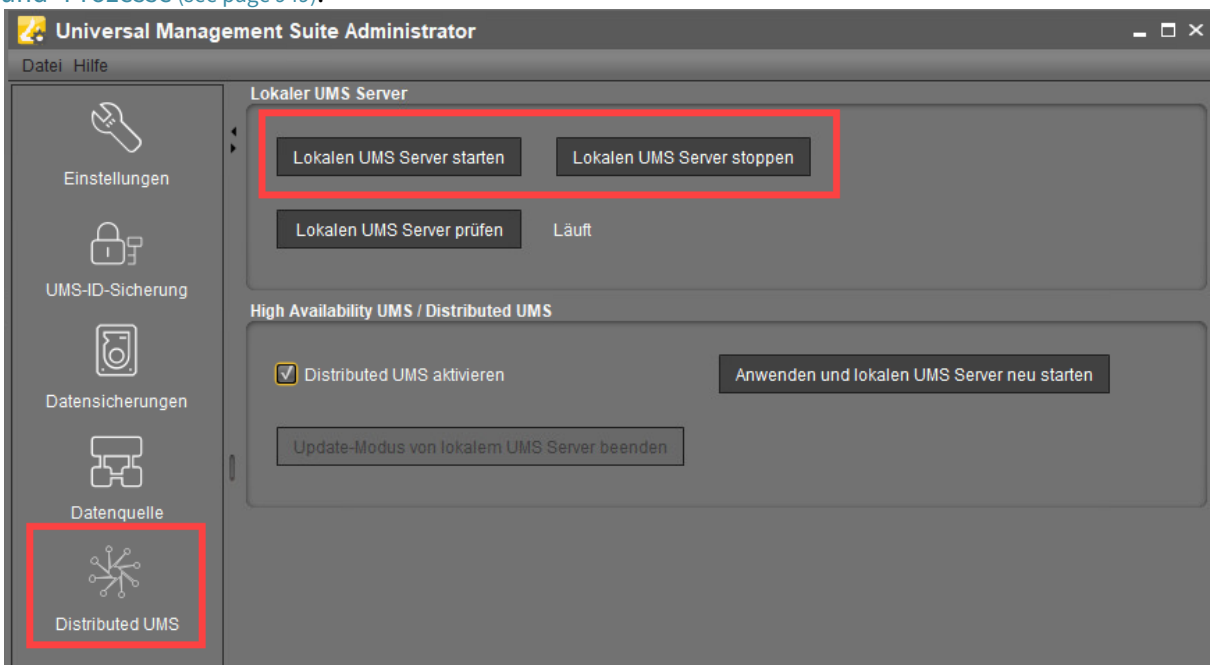
2. Kopieren Sie die eingebettete Datenbank in die neue externe Datenquelle, siehe Datenquelle kopieren (see page 735), und **aktivieren** Sie die neue Datenquelle.

3. Öffnen Sie die UMS Konsole und gehen Sie zu **UMS Administration > UMS Netzwerk > Server**, um zu prüfen, ob der Server läuft.

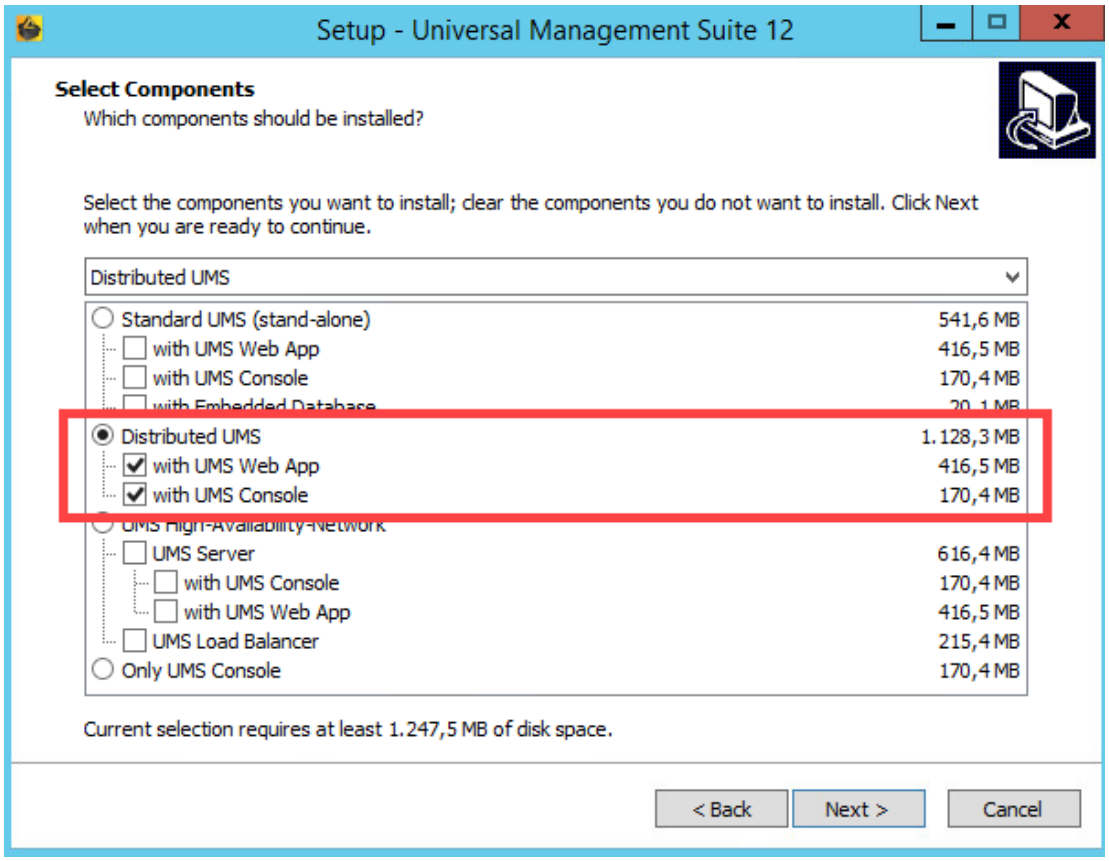
4. Gehen Sie zu **UMS Administration > Globale Konfiguration > Server-Netzwerkeinstellungen** und aktivieren Sie **Distributed UMS aktiviert**.



5. Starten Sie den UMS Server-Dienst neu, z. B. über **UMS Administrator > Distributed UMS** (see page 738). Eine ausführliche Anleitung zum Neustart von Diensten finden Sie unter IGEL UMS HA-Dienste und -Prozesse (see page 949).



6. Installieren Sie weitere UMS Server (dabei aktivieren Sie **Distributed UMS** im UMS Installer) und verbinden Sie sie mit derselben Datenbank.



⚠ Wenn Sie die Distributed UMS-Funktion aktiviert haben und über mehrere UMS Server verfügen, seien Sie vorsichtig, falls Sie die Funktion deaktivieren möchten. Wenn die Distributed UMS-Funktion deaktiviert wird, aber mehrere UMS Server dieselbe Datenbank verwenden, wird keine Synchronisierung zwischen den UMS Servern durchgeführt.

Leitlinien zur Installation und Größenbestimmung der IGEL UMS

Die folgenden Empfehlungen und Größenangaben sollen Sie bei der Einrichtung der IGEL UMS Umgebung, d.h. UMS Server, UMS Konsole / Web App, Datenbank und, falls erforderlich, Load Balancer sowie ICG Instanzen, unterstützen. Informationen zu den Installationsanforderungen finden Sie unter Installationsvoraussetzungen für die IGEL UMS (see page 250).

Die Größe und Struktur der UMS Installation hängt hauptsächlich von den folgenden Kriterien ab:

- Anzahl der Geräte
- High Availability
- ICG Verbindung für Geräte außerhalb Ihres Unternehmensnetzwerks

Allgemeine Voraussetzungen

Die Installations- und Größenangaben gelten für eine Standard UMS Installation und beschreiben die gängigsten UMS Umgebungen. Einzelne Ausnahmen oder Anforderungen werden durch diese Szenarien möglicherweise nicht abgedeckt.

- Systemanforderungen: UMS 6.05 und neuer, ICG 2.02 und neuer
- UMS Konsole kann sich **innerhalb desselben (V)LANs wie die UMS Server** befinden (kein NAT, keine Proxies) oder **außerhalb des VLANs** mit Firewalls/Routing, die gemäß IGEL UMS Kommunikationsports (see page 6) konfiguriert sind.
- Geräte, **die direkt mit dem UMS Server verbunden** sind, befinden sich **im selben (V)LAN wie die UMS Server** (kein NAT, keine Proxys). Falls eine Firewall verwendet wird, muss diese gemäß IGEL UMS Kommunikationsports (see page 6) konfiguriert werden.
- Geräte **außerhalb des internen LANs** sind **über ICG** verbunden.
- Die Geräte **werden nicht häufig gebootet bzw. neu gestartet** (durchschnittlich einmal pro Tag).
- **Maximal 10 verschiedene Firmware-Versionen** werden über die UMS verwaltet.
- UMS Backups und Exporte werden **nicht dauerhaft auf dem UMS-Server-Host** gespeichert.
- Im Falle der automatischen Geräteregistrierung (siehe Geräte automatisch an der IGEL UMS registrieren (see page 337)): Der **DNS**-Alias `igelrmserver` oder das **DHCP**-Tag können nur auf EINE UMS Installation zeigen. Daher ist die Installation mehrerer separater UMS Server (ohne die High-Availability-Erweiterung) in einem Netzwerk nicht zu empfehlen.

  ⚠
  - High Availability mit IGEL UMS Load Balancern: Alle UMS Server und UMS Load Balancer müssen sich im **selben VLAN** befinden.
  - Für High Availability (UMS HA) mit IGEL UMS Load Balancern muss der Netzwerkverkehr über den UDP-Broadcast-Port 6155 und der TCP-Verkehr sowie UDP-Broadcast-Verkehr über Port 61616 zugelassen werden. Weitere Informationen zu den UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).
  - In der Netzwerkkonfiguration auf Windows-Servern muss die Option TCP/IPv6 für UMS 12 aktiviert sein.

- IGEL UMS HA Installation mit IGEL UMS Load Balancern wird in Cloud-Umgebungen wie Azure / AWS nicht unterstützt, da sie keinen Broadcast-Verkehr innerhalb ihrer Netzwerke zulassen. Die HA-Installation ohne IGEL UMS Load Balancer (sowie die Distributed UMS (see page 246)) wird jedoch in Cloud-Umgebungen ab UMS Version 6.10 unterstützt.

Wir empfehlen Ihnen folgende zusätzliche Informationen:

IGEL UMS Kommunikationsports (see page 6): Hier finden Sie eine Liste mit allen Ports, die für die Kommunikation mit der UMS relevant sind.
"Supported Environment": In diesem Abschnitt der aktuellen Release Notes (see page 965) können Sie nachlesen, welche Server, Clients und Backend-Datenbanken unterstützt werden.
High Availability (HA) (see page 909): Hier finden Sie nützliche Anleitungen und das Referenzhandbuch rund um Ihre HA-Installation.
IGEL Cloud Gateway: Hier finden Sie Anleitungen, das Referenzhandbuch und zusätzliche Informationen zur Verwaltung von Endgeräten außerhalb des Unternehmensnetzwerks.

- IGEL UMS Größenangaben & Architekturdiagramme (see page 281)
- Leistungsoptimierungen (see page 294)
- IGEL Cloud Gateway vs. Reverse Proxy for the Communication between UMS 12 and IGEL OS Devices (see page 297)

IGEL UMS Größenangaben & Architekturdiagramme

Die folgenden Empfehlungen und Größenangaben sollen Sie bei der Einrichtung der IGEL UMS Umgebung, d.h. UMS Server, UMS Konsole / Web App, Datenbank und, falls erforderlich, Load Balancer sowie ICG Instanzen, unterstützen.

Allgemeine Installationsempfehlungen
Für kleine Installationen ist in der Regel eine einzelne UMS Server-Instanz ("Standard UMS") mit einer eingebetteten Datenbank ausreichend. Bei Bedarf kann eine Einzelinstanz-Installation jederzeit durch die Installation zusätzlicher Server zu einer Distributed UMS Installation erweitert werden (im Falle einer eingebetteten Datenbank ist auch der Umstieg auf eine externe Datenquelle nötig).
Große Installationen sollten entweder die UMS High Availability oder die Distributed UMS (bevorzugt bei Neuinstallationen, da z. B. keine zusätzlichen Firewallausnahmen konfiguriert werden müssen) verwenden. Für große Installationen wird auch der Einsatz von DNS-Round-Robin-Lastverteilung oder IGEL Cloud Gateway empfohlen.
Mehr Informationen finden Sie unter IGEL UMS Installation (see page 246).

Größe der Installation	#Geräte	#UMS Server Host (+ Load Balancer)	UMS Server	UMS Konsole (standalone)	#Load Balancer (standalone)	Load Balancers (standalone)	Datenbank**	ICG
S	**< 5.000**	**1 Server**	8 GB RAM (UMS Web App + 1 GB) 4 CPUs 25 GB freier Speicherplatz	**Optional*** 3 GB RAM 2 CPUs 1 GB freier Speicherplatz			Embedded-Datenbank	**1 ICG Instanz pro 2,500 Geräte** **Server generell:** 8 GB RAM 2 CPUs 20 GB freier Speicherplatz **Nur ICG Dienst:** 4 GB RAM 2 CPUs 2 GB freier Speicherplatz
M	**< 15.000**	**1 Server**	8 GB RAM (UMS Web App + 1 GB) 4 CPUs 25 GB freier Speicherplatz	**Optional*** 3 GB RAM 2 CPUs 1 GB freier Speicherplatz			**Externe Datenbank** 10 GB	
M / S (HA oder Distributed UMS)	**< 15.000**	**2 Server** **2 Load Balancer**	9 GB RAM (Web App +1GB) 6 CPUs 25 GB freier Speicherplatz	**Optional*** 3 GB RAM 2 CPUs 1 GB freier Speicherplatz			**Externe Datenbank** 10 GB	
L (HA oder Distributed UMS)	**< 50.000**	**2 Server** **2 Load Balancer**	6 GB RAM*** (Web App +1GB) 4 CPUs 25 GB freier Speicherplatz	**Obligatorisch** 3 GB RAM 2 CPUs 1 GB freier Speicherplatz			**Externe Datenbank** 10 GB	

Größe der Installation	#Geräte	#UMS Server Host (+ Load Balancer)	UMS Server	UMS Konsole (standalone)	#Load Balancer (standalone)	Load Balancers (standalone)	Datenbank**	ICG
XL (HA oder Distributed UMS)* ***	**< 300.000**	**Bis zu 6 Server** (1 Server / 50,000 Geräte)	9 GB RAM (Web App +1GB) 6 CPUs 25 GB freier Speicherplatz	**Obligatorisch** 6 GB RAM 4 CPUs 1 GB freier Speicherplatz	Bis zu 3 Load Balancer (1 LB / 3 Server)	4 GB RAM 4 CPUs 2 GB freier Speicherplatz	**Externe Datenbank** 20 GB	

* Die UMS Konsole kann auf dem UMS Server-Host installiert werden.

** Befolgen Sie die Empfehlung des externen Datenbanksystems für RAM und CPU.

*** Die RAM- und CPU-Anforderungen sind geringer als bei einer **M / S (HA)**-Installation, da die UMS Konsole auf einem separaten Host installiert wird (**UMS Konsole (standalone)** = **Obligatorisch**).

**** Allgemeine Empfehlung: 1 UMS Server pro 50.000 Geräte, 1 Load Balancer für 3 UMS Server.

Die Architekturdiagramme der Installations finden Sie unter:

- Kleine Umgebung: UMS S (see page 284)
- Mittelgroße Umgebung: UMS M (see page 286)
- Kleine und mittelgroße Umgebungen: UMS M/S (HA) (see page 288)
- Große Umgebung: UMS L (HA) (see page 290)
- Besonders große Umgebung: UMS XL (HA) (see page 292)

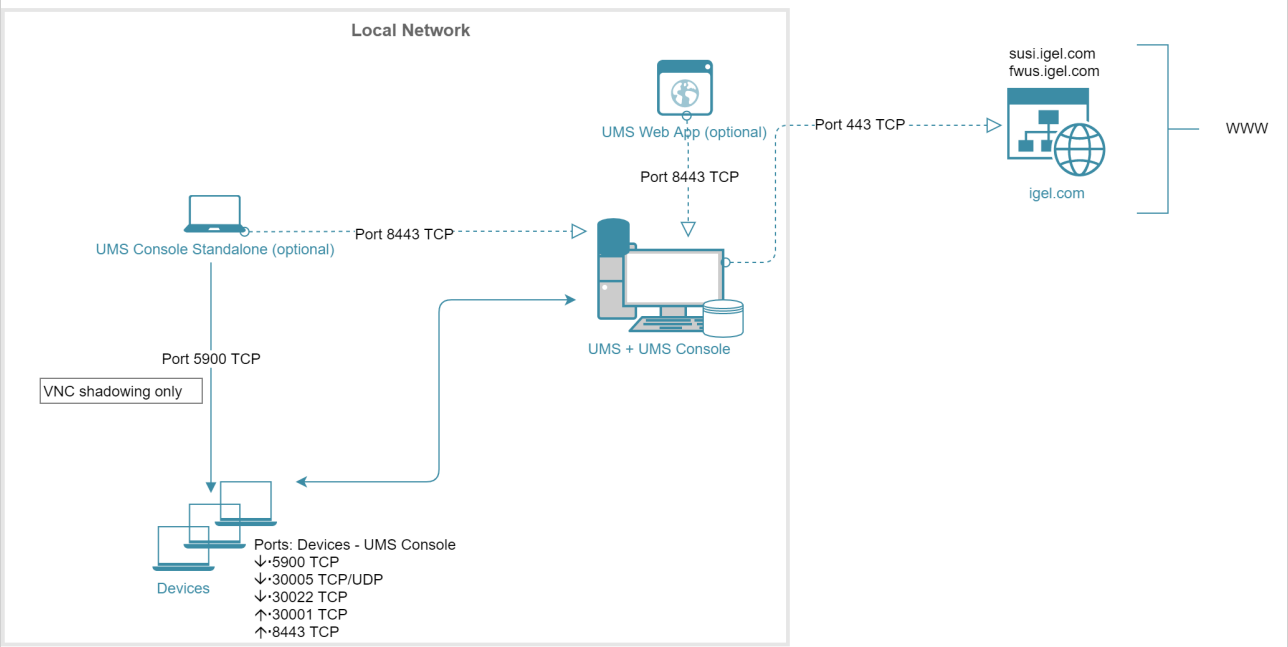
Kleine Umgebung: UMS S

Kleine UMS Installation (<5k Geräte) oder Demo/POV Umgebung mit einer Embedded-Datenbank

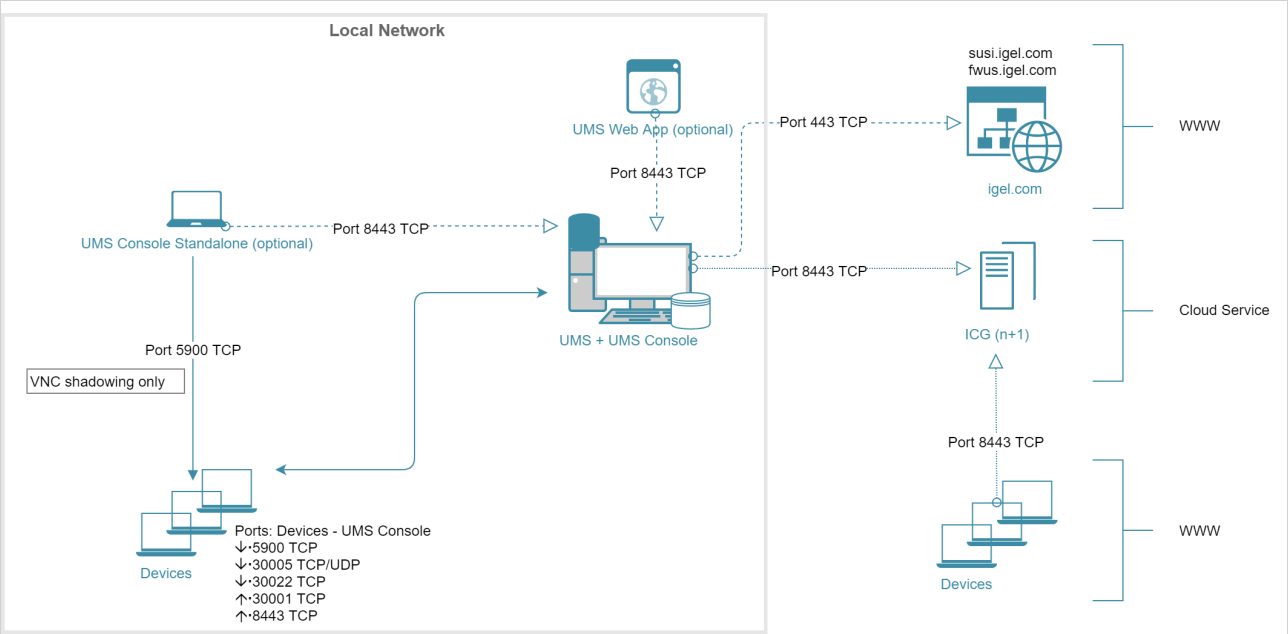
Installation	#Geräte	#UMS Server Host	UMS Server	UMS Konsole (standalone)	#Load Balancer (standalone)	Load Balancer (standalone)	Datenbank	ICG
S	< **5.000**	**1 Server**	8 GB RAM (UMS Web App + 1 GB) 4 CPUs 25 GB freier Speicherplatz	**Optional*** 3 GB RAM 2 CPUs 1 GB HDD			Embedded-Datenbank	**1 ICG-Instanz pro 2,500 Geräte** **Server generell:** 8 GB RAM 2 CPUs 20 GB HDD **Nur ICG-Dienst:** 4 GB RAM 2 CPUs 2 GB HDD

***** Die UMS Konsole kann auf dem Host eines UMS Servers installiert werden.

Architektur: Kleine Umgebung



Architektur: Kleine Umgebung + ICG in der Cloud



Mittelgroße Umgebung: UMS M

Mittelgroße UMS Installationen (bis zu ~15k Geräten); keine High Availability

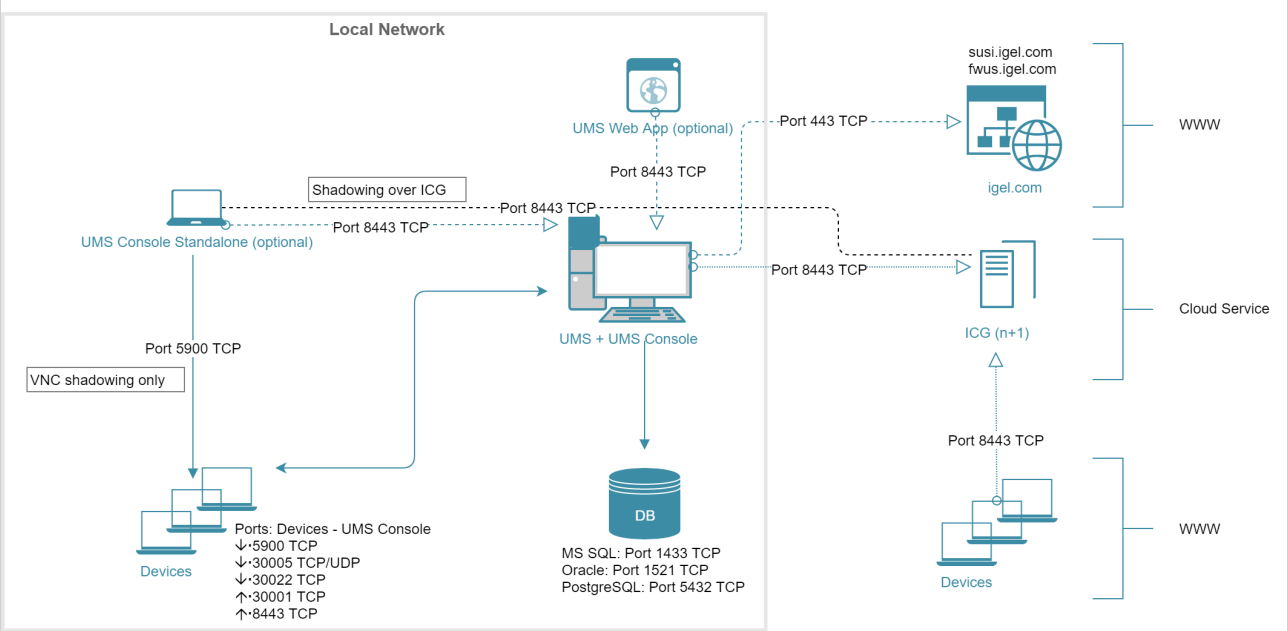
Installation	#Geräte	#UMS Server Host	UMS Server	UMS Konsole (standalone)	#Load Balancer (standalone)	Load Balancer (standalone)	Datenbank**	ICG
M	**< 15.000**	**1 Server**	8 GB RAM (UMS Web App + 1 GB) 4 CPUs 25 GB freier Speicherplatz	**Optional*** 3 GB RAM 2 CPUs 1 GB HDD			**Externe Datenbank** 10 GB	**1 ICG-Instanz pro 2,500 Geräte** **Server generell:** 8 GB RAM 2 CPUs 20 GB HDD **Nur ICG-Dienst:** 4 GB RAM 2 CPUs 2 GB HDD

***** Die UMS Konsole kann auf dem Host des UMS Servers installiert werden.

****** Befolgen Sie die Empfehlung des externen Datenbanksystems für RAM und CPU.

Zu High Availability in dieser Umgebung siehe Kleine und mittelgroße Umgebungen (HA) (see page 288).

Architektur: Mittelgroße Umgebung + ICG


Local Network
UMS Web App (optional)
Port 443 TCP
susi.igel.com
fwus.igel.com
igel.com
WWW
Port 8443 TCP
Shadowing over ICG
Port 8443 TCP
Port 8443 TCP
UMS Console Standalone (optional)
Port 8443 TCP
UMS + UMS Console
ICG (n+1)
Cloud Service
Port 5900 TCP
VNC shadowing only
Port 8443 TCP
DB
Devices
Ports: Devices - UMS Console
↓·5900 TCP
↓·30005 TCP/UDP
↓·30022 TCP
↑·30001 TCP
↑·8443 TCP
MS SQL: Port 1433 TCP
Oracle: Port 1521 TCP
PostgreSQL: Port 5432 TCP
Devices
WWW

Kleine und mittelgroße Umgebungen: UMS M/S (HA)

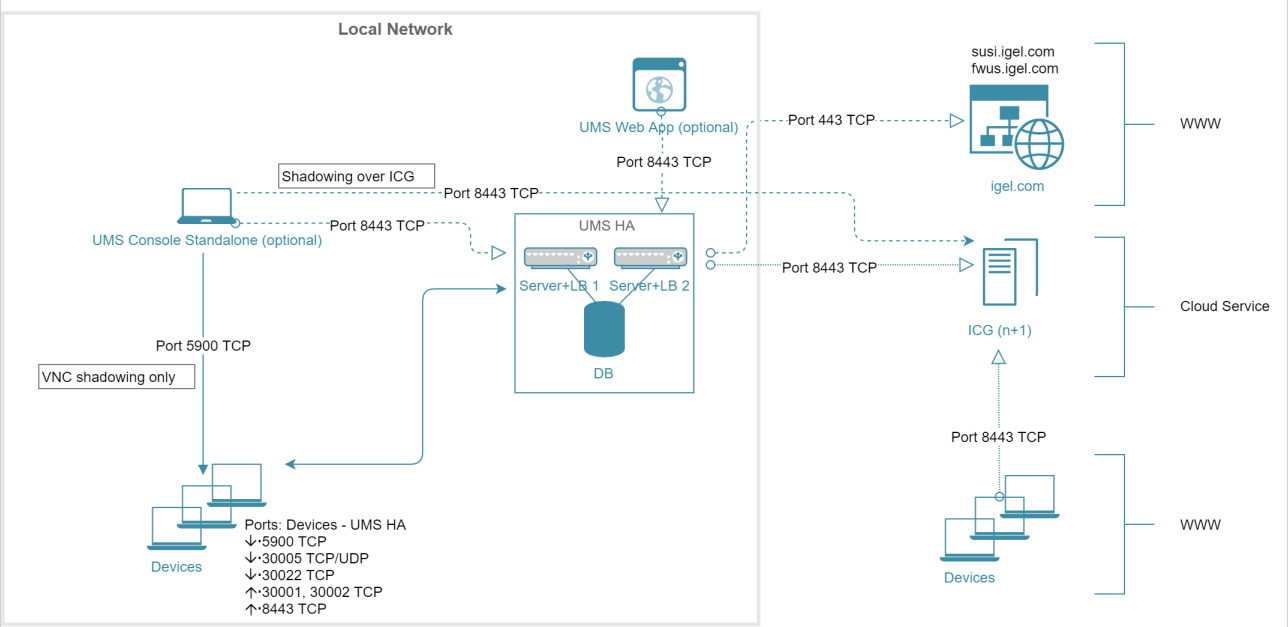
Kleine und mittelgroße UMS Installationen (bis zu ~15k Geräten); High Availability (HA)

Installation	#Geräte	#UMS Server Host (+ Load Balancer)	UMS Server	UMS Konsole (standalone)	#Load Balancer (standalone)	Load Balancer (standalone)	Datenbank**	ICG
M / S (HA oder Distributed UMS (see page 246)**)**	**< 15.000**	**2 Server** **2 Load Balancer**	9 GB RAM (Web App +1GB) 6 CPUs 25 GB HDD	**Optional*** 3 GB RAM 2 CPUs 1 GB HDD			**Externe Datenbank** 10 GB	**1 ICG-Instanz pro 2,500 Geräte** **Server generell:** 8 GB RAM 2 CPUs 20 GB HDD **Nur ICG-Dienst:** 4 GB RAM 2 CPUs 2 GB HDD

***** Die UMS Konsole kann auf dem Server des UMS Servers installiert werden.

****** Befolgen Sie die Empfehlung des externen Datenbanksystems für RAM und CPU.

Architektur: Kleine und mittelgroße Umgebungen (HA) + ICG


Local Network
UMS Web App (optional)
Port 443 TCP
susi.igel.com
fwus.igel.com
WWW
igel.com
Port 8443 TCP
Shadowing over ICG
Port 8443 TCP
UMS Console Standalone (optional)
Port 8443 TCP
UMS HA
Server+LB 1
Server+LB 2
DB
Port 8443 TCP
Cloud Service
ICG (n+1)
Port 5900 TCP
VNC shadowing only
Port 8443 TCP
Devices
Ports: Devices - UMS HA
↓·5900 TCP
↓·30005 TCP/UDP
↓·30022 TCP
↑·30001, 30002 TCP
↑·8443 TCP
Devices
WWW

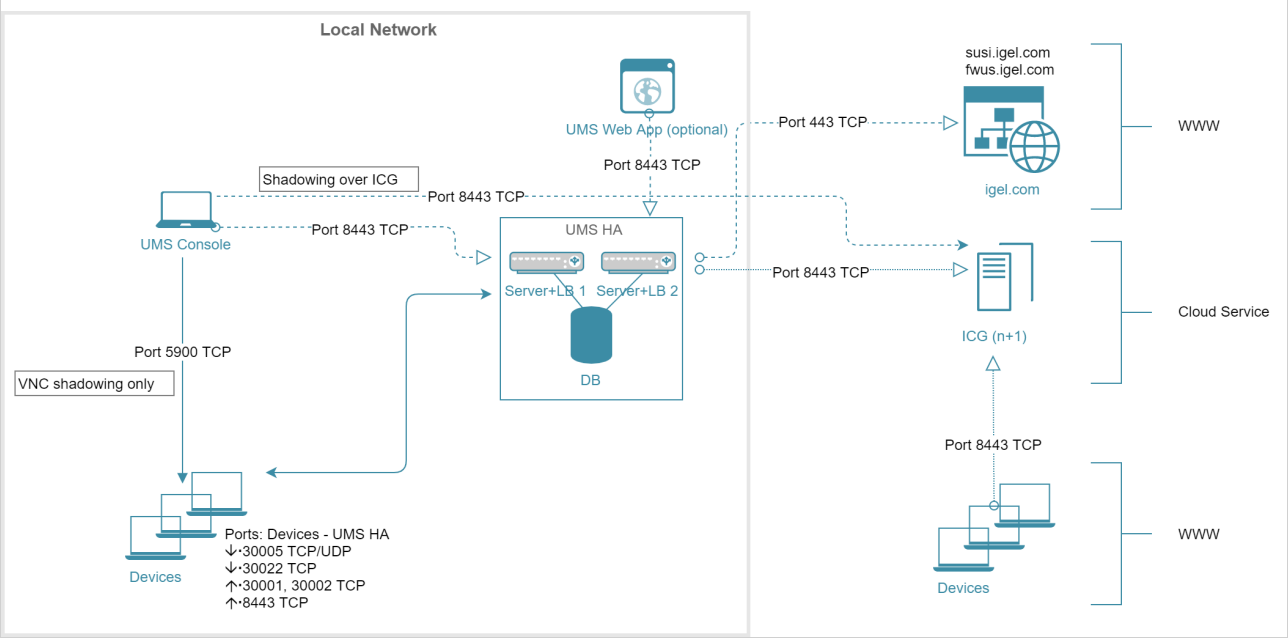
Große Umgebung: UMS L (HA)

Große UMS Installationen mit bis zu 50k Geräten; High Availability (HA) + ICG

Installation	#Geräte	#UMS Server Host (+ Load Balancer)	UMS Server	UMS Konsole (standalone)	#Load Balancer (standalone)	Load Balancer (standalone)	Datenbank*	ICG
L (HA oder Distributed UMS (see page 246)**)**	**< 50.000**	**2 Server** **2 Load Balancer**	6 GB RAM (Web App +1GB) 4 CPUs 25 GB HDD	**Obligatorisch** 3 GB RAM 2 CPUs 1 GB HDD			**Externe Datenbank** 10 GB	**1 ICG-Instanz pro 2,500 Geräte** **Server generell:** 8 GB RAM 2 CPUs 20 GB HDD **Nur ICG-Dienst:** 4 GB RAM 2 CPUs 2 GB HDD

***** Befolgen Sie die Empfehlung des externen Datenbanksystems für RAM und CPU.

Architektur: Große Umgebung (HA) + ICG


Local Network
UMS Web App (optional)
Port 443 TCP
susi.igel.com
fwus.igel.com
WWW
Port 8443 TCP
Shadowing over ICG
Port 8443 TCP
igel.com
UMS Console
Port 8443 TCP
UMS HA
Server+LB 1
Server+LB 2
Port 8443 TCP
Cloud Service
ICG (n+1)
Port 5900 TCP
VNC shadowing only
DB
Port 8443 TCP
Devices
Ports: Devices - UMS HA
↓·30005 TCP/UDP
↓·30022 TCP
↑·30001, 30002 TCP
↑·8443 TCP
Devices
WWW

Besonders große Umgebung: UMS XL (HA)

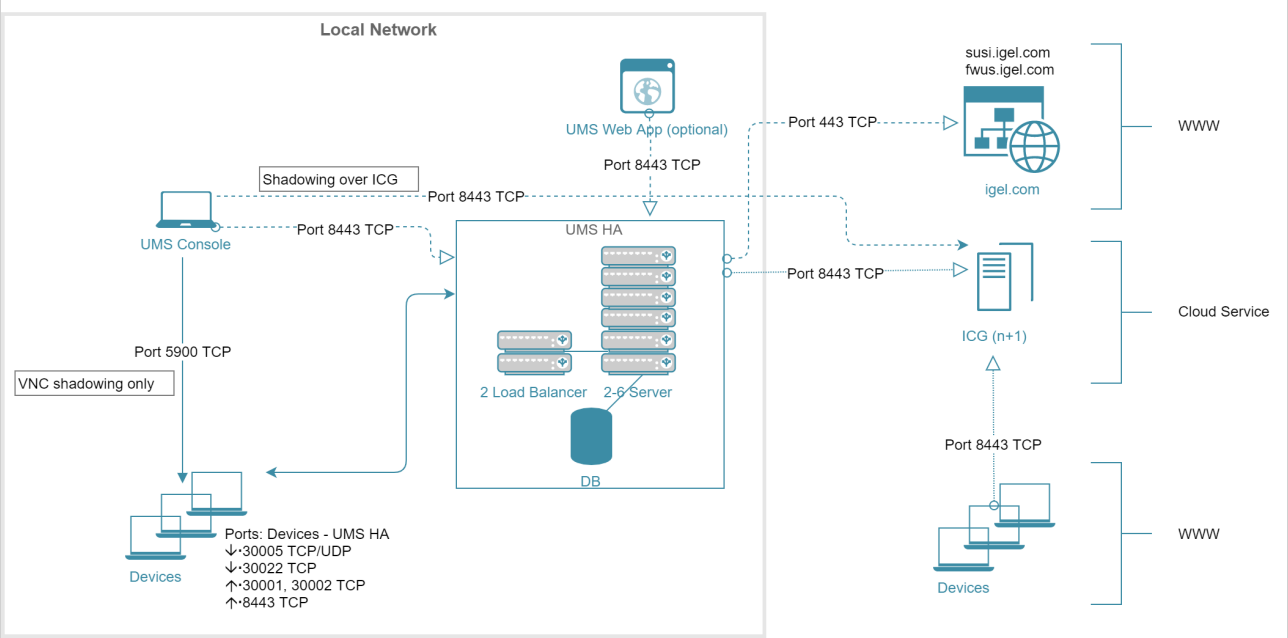
Besonders große UMS Installationen mit bis zu 300k Geräten; High Availability (HA) + ICG

Installation	#Geräte	#UMS Server Host	UMS Server	UMS Konsole (standalone)	#Load Balancer (standalone)	Load Balancer (standalone)	Datenbank*	ICG
XL (HA oder Distributed UMS (see page 246)**)****	**< 300.000**	**Bis zu 6 Server** (1 Server / 50,000 Geräte)	9 GB RAM (Web App +1GB) 6 CPUs 25 GB HDD	**Obligatorisch** 6 GB RAM 4 CPUs 1 GB HDD	Bis zu 3 Load Balancer (1 LB / 3 Server)	4 GB RAM 4 CPUs 2 GB HDD	**Externe Datenbank** 20 GB	**1 ICG-Instanz pro 2,500 Geräte** **Server generell:** 8 GB RAM 2 CPUs 20 GB HDD **Nur ICG-Dienst:** 4 GB RAM 2 CPUs 2 GB HDD

***** Befolgen Sie die Empfehlung des externen Datenbanksystems für RAM und CPU.

****** Allgemeine Empfehlung: 1 UMS Server pro 50.000 Geräte, 1 Load Balancer für 3 UMS Server.

Architektur: Besonders große Umgebung (HA) + ICG


Local Network
UMS Web App (optional)
Port 443 TCP
susi.igel.com
fwus.igel.com
WWW
Port 8443 TCP
Shadowing over ICG
Port 8443 TCP
igel.com
UMS Console
Port 8443 TCP
UMS HA
Port 8443 TCP
Cloud Service
ICG (n+1)
Port 5900 TCP
VNC shadowing only
2 Load Balancer
2-6 Server
DB
Port 8443 TCP
Devices
Ports: Devices - UMS HA
↓·30005 TCP/UDP
↓·30022 TCP
↑·30001, 30002 TCP
↑·8443 TCP
Devices
WWW

Leistungsoptimierungen

Datengrößen

- Die Anzahl der registrierten Firmwareversionen hat den **größten Einfluss** auf die Größe der Datenbank.
  (In der UMS Konsole zu finden unter **Extras > Firmwarestatistik**)
- Die Anzahl der Geräte hat einen **kleineren Einfluß**.
- Durchschnittliche Größe pro...
  - Firmwarekonfiguration: ~15 MB
  - Profile (abhängig von der Anzahl aktiver Parameter): ~100 kB
  - Geräte: ~100 kB
- Reservieren Sie 500 MB bis 1 GB für Datenbank-Transaktionsprotokolle von übermäßigen Datenbankaufrufen wie **Unbenutzte Firmwares entfernen**. Bitte beachten Sie, dass die Verwendung vom jeweiligen Datenbanksystem abhängt.

Latenzzeiten

Wenn Sie mit Fernverbindungen und hohen Latenzzeiten zu kämpfen haben, beachten Sie bitte die folgenden Empfehlungen:

- Minimieren Sie die Latenzzeiten zwischen...
  - Datenbank <-> UMS Server: <= 20 ms
  - verschiedenen UMS Servern: <= 50 ms
  - Load Balancer <-> UMS Server: <= 50 ms
- Eine hohe Latenzzeit zwischen der Datenbank und dem UMS Server hat einen **großen Einfluss** auf die Leistung. Die Kommunikation zwischen dem Gerät und der UMS Konsole wird langsamer, die UMS Konsole reagiert träge.
- Eine hohe Latenzzeit zwischen dem Gerät und dem UMS Server hat **wenig Einfluss** auf die Gesamtleistung.

Optimierungen der Leistung

- **UMS Protokolldaten:**
  Verwenden Sie administrative Aufgaben (see page 597) zur automatischen Bereinigung von Protokollen (Logging-Informationen, Ergebnisse von Aufgaben, Ergebnisse von administrativen Aufgaben, Prozessereignisse, Verlauf der Assetinformationen) oder entfernen Sie alte UMS Protokolldateien (`/rmguiserver/logs`), wenn der Speicherplatz knapp wird.
- **Firmware:**
  Unbenutzte Firmware regelmäßig entfernen.
- **Nur Embedded-Datenbank:**
  - Datenbank regelmäßig optimieren (UMS Administrator, z.B. einmal pro Monat).
  - Prüfen Sie auf freien Festspeicherplatz und erweitern Sie den Festspeicher, falls erforderlich (halten Sie immer mindestens 1 GB frei).
- **Anzahl Geräte:**

    - Wenn die Anzahl der Geräte hoch (>10k) und die Gesamtleistung niedrig ist, erhöhen Sie den Arbeitsspeicher von UMS Server und UMS Konsole.
    - Es sollten sich nicht zu viele Geräte (>5k) in in einem Ordner befinden.
- **Zuweisungen:**
  Halten Sie die Anzahl der Zuweisungen pro Gerät (direkt und indirekt) niedrig (<25).
- **Administrative Aufgaben und Jobs:**
  Je mehr administrative Aufgaben und Jobs erstellt werden, desto mehr Heap wird verbraucht, daher kann es notwendig sein, den Speicher für den UMS Server zu vergrößern. Siehe Wie konfiguriere ich die Java-Heap-Größe für den UMS Server? (see page 141).
- **Vorgabeverzeichnisse:**
  Verwenden Sie keine Vorgabeverzeichnisse mit der Option **Regel anwenden, wenn das Gerät gebootet wird**, wenn nicht anders verlangt.
- **Gleichzeitige Geräteanfrangen:**
  Wenn Sie Probleme mit vielen gleichzeitigen Geräteanfragen haben (Verzögerungen bei der Konfigurationsbereitstellung oder Anmeldung am Gerät), verwenden Sie in der UMS Konsole die Optionen **UMS Administration > Globale Konfiguration > Geräte-Netzwerkeinstellungen > Geräteanfragen** (Thread- und Warteschlangengröße), um den Durchsatz der Geräteanforderungen zu steuern. Wenden Sie sich für Empfehlungen an den Support.

Grenzen: UMS HA

- Geräteaktionen, die manuell in der UMS Konsole ausgelöst werden, werden von **einem UMS Server** ausgeführt (derjenige, mit dem die UMS Konsole derzeit verbunden ist); für diese Aktionen gibt es keinen Lastausgleich.

IGEL UMS Maintenance Tasks

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

IGEL Cloud Gateway vs. Reverse Proxy for the Communication between UMS 12 and IGEL OS Devices

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

UMS aktualisieren

Hier erfahren Sie, wie Sie die IGEL Universal Management Suite (UMS) unter Windows oder Linux aktualisieren. Eine Update-Anleitung für die UMS High-Availability-Installation finden Sie unter Installation eines HA-Netzwerks aktualisieren (see page 931).

Update-Anleitung

- IGEL UMS unter Linux aktualisieren (see page 300)
- IGEL UMS unter Windows aktualisieren (see page 304)

Update-Vorbereitung

⚠ Überprüfen Sie vor der Installation, ob Ihre Hardware und Software die Installationsvoraussetzungen erfüllen, siehe Installationsvoraussetzungen für die IGEL UMS (see page 250). Siehe auch Geräte, die von der IGEL Universal Management Suite (UMS) unterstützt werden (see page 5).

⚠ Erstellen Sie ein Backup der Datenbank, bevor Sie eine zuvor installierte Version der UMS aktualisieren. Ansonsten droht Verlust aller Datenbankinhalte. Siehe Datensicherungen (see page 719) und Ein Backup der IGEL UMS erstellen (see page 720).

✔ Wir empfehlen, die neue Version der UMS vor der Installation im Produktivsystem in einem Testsystem zu installieren. Wenn Sie die Funktionen der neuen Version im Testsystem überprüft haben, können Sie die neue Version im Produktivsystem installieren. Dies trifft auch für Hotfixes, Patches usw. von Serversystem und Datenbank zu.

⚠ Die Installation einer älteren als der aktuell verwendeten UMS Version ist nur dann möglich, wenn Sie ein Backup der Datenbank mit dem passenden älteren Schema haben. Sie können nur von einem älteren Datenbankschema auf ein neueres wechseln, nicht umgekehrt. Erstellen Sie daher ein Backup von Ihrem laufenden System, bevor Sie mit der Aktualisierung beginnen.
Da die Version des Datenbankschemas immer der aktuellen Major.Minor-Version der UMS entspricht (d.h. 6.10 für alle 6.10.x-Releases, 6.08 für alle 6.08.x-Releases), sind Downgrades nur innerhalb einer Major.Minor-Version möglich. Beispiel: Sie können ein Downgrade von 6.10.140 auf 6.10.120 durchführen, aber nicht von 6.10.140 auf 6.09.120.

⚠ Wenn die Version der UMS Konsole älter ist als die Version des UMS Servers, können Sie keine Verbindung zum Server herstellen (Fehlermeldung `Unable to load tree`). In diesem Fall müssen Sie die Installation der UMS Konsole aktualisieren.

WebDAV-Downloads (z. B. Dateien, Firmwareupdates) werden im Verzeichnis `ums_filetransfer` gespeichert. Frei wählbare Verzeichnisse für Dateiübertragungen werden nicht unterstützt.

Während des Upgrades der UMS, z. B. von der Version 6.09 auf 6.10 oder von der Version 6.x auf 12.x, wird das Datenbankschema durch den Installer geändert. Bei großen Produktionsdatenbanken kann dieser Prozess bis zu 2 Stunden dauern. Brechen Sie die Installation während dieser Zeit nicht ab.

IGEL UMS unter Linux aktualisieren

Bevor Sie ein Update der IGEL Universal Management Suite (UMS) starten, lesen Sie UMS aktualisieren (see page 298).

⚠ Erstellen Sie ein Backup der Datenbank (see page 719), bevor Sie eine zuvor installierte Version der UMS aktualisieren. Ansonsten droht Verlust aller Datenbankinhalte.

⚠ **Oracle**

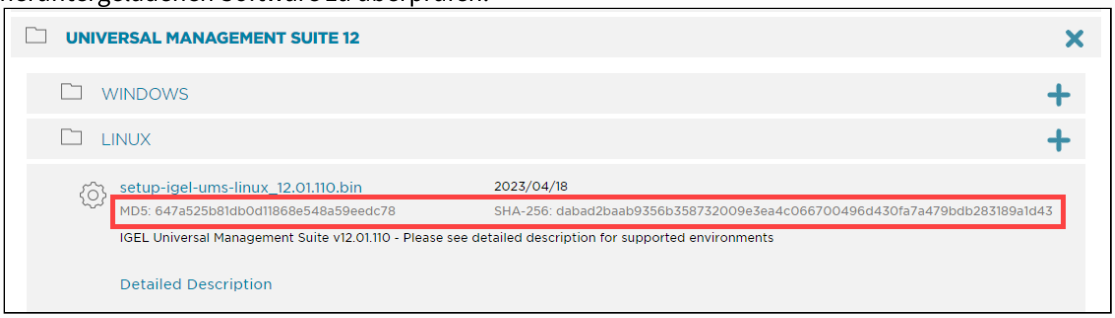
Für den ordnungsgemäßen Betrieb der UMS mit Oracle-Datenbanken, insbesondere für den Aktualisierungsvorgang, muss die Anzahl von `open_cursors` für die Datenbank angepasst werden. `open_cursors` ist eine Systemeinstellung.

1. Um den aktuellen Wert zu erfahren, melden Sie sich als `SYSDBA` an der Datenbank an und führen Sie aus:
   `SQL> select name, value from v$parameter where name = 'open_cursors';`
2. Der empfohlene Wert für `open_cursors` ist "3000". Um den Wert zu setzen, führen Sie den folgenden Befehl als `SYSDBA` aus:
   `SQL> alter system set open_cursors = 3000 scope=both;`
3. Der gleiche Befehl sollte der `SPFILE` des Oracle-Systems hinzugefügt werden, damit die Änderungen beim nächsten Neustart erhalten bleiben.

So führen Sie ein Update unter Linux aus:

1. Laden Sie die aktuelle Version der IGEL Universal Management Suite vom IGEL Downloadserver[20] herunter.

   ⓘ Aus Integritäts- und Sicherheitsgründen empfiehlt es sich, die Prüfsumme (Checksum) der heruntergeladenen Software zu überprüfen.



20 https://www.igel.com/software-downloads/

2. Öffnen Sie einen Terminalemulator wie beispielsweise xterm und wechseln Sie in das Verzeichnis, in dem sich die Installationsdatei `setup-igel-ums-linux-[Version].bin` befindet.

3. Überprüfen Sie, ob die Datei ausführbar ist. Falls nicht, lässt sie sich mit folgendem Befehl ausführbar machen:
   `chmod u+x setup*.bin`

   > Sie brauchen root/sudo-Rechte, um die Installation durchzuführen.

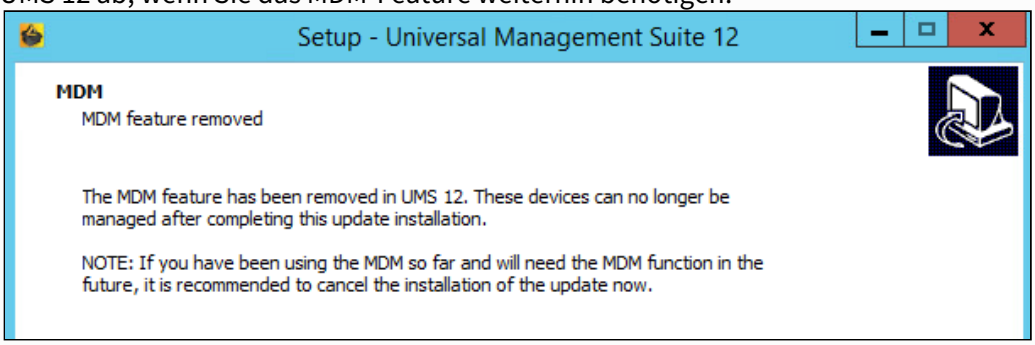
4. Führen Sie die Installationsdatei als `root` oder mit `sudo` aus.
   `sudo ./setup-igel-ums-linux-[Version].bin`
   Der Installer entpackt die Dateien ins Verzeichnis `/tmp`, startet die enthaltene Java Virtual Machine und entfernt die temporären Dateien nach dem Installationsvorgang.

5. Starten Sie den Installationsvorgang mit **Enter**.

   > Sie können die Installation jederzeit durch zweimaliges Drücken der Taste [Esc] abbrechen.

6. Lesen und bestätigen Sie die Lizenzvereinbarung.

7. Wählen Sie unter **Database backup** eine Datei für das Backup der existierenden Embedded-Datenbank. Falls Sie bereits ein Backup erstellt haben, können Sie auch **No (continue)** wählen, um diesen Schritt zu überspringen.

   > **Nur für Update-Installationen**
   > - Ab UMS 12 ist das MDM-Feature nicht mehr verfügbar. Brechen Sie das Upgrade auf UMS 12 ab, wenn Sie das MDM-Feature weiterhin benötigen:
   >
   > 
   >
   >
   > - Nur wenn Sie eine Distributed UMS-Installation haben: Während der Update-Installation wird geprüft, ob nur ein UMS Server läuft und die anderen gestoppt sind. Wenn dies nicht der Fall ist, stoppen Sie alle UMS Server bis auf einen und fahren Sie mit der Aktualisierung fort; andernfalls riskieren Sie einen Datenverlust.

Nachdem die Aktualisierung auf diesem Server abgeschlossen ist, können Sie die übrigen UMS Server aktualisieren, entweder parallel oder nacheinander.

8. Wählen Sie unter **Installation type** den Installationsumfang:
   - **Complete**: UMS Server und UMS Konsole
   - **Distributed UMS**: Distributed UMS-Installation (see page 246)
   - **HA net**: High-Availability (see page 909)-Konfiguration
   - **Client only**: nur UMS Konsole

9. Wählen Sie, ob die IGEL UMS Web App (see page 783) installiert werden soll. Siehe Wichtige Informationen zur IGEL UMS Web App (see page 784).

10. Bestätigen Sie den Dialog, dass Ihr System die angezeigten **Systemanforderungen** erfüllt.

11. Bestätigen oder geben Sie die IP-Adresse des UMS Servers unter **Confirm server IP address** ein. Diese IP-Adresse wird für die Erstellung des UMS Server-Zertifikats beim ersten Start verwendet. Dieser Dialog wird nur bei der ersten Installation einer UMS-Version angezeigt, die dieses Feature beinhaltet.

    ⚠ Wenn Sie bei der Installation der UMS die IP-Adresse nicht anpassen, enthält das Webzertifikat Ihres UMS Servers die inkorrekte IP-Adresse, was zu Problemen bei der Geräteregistrierung usw. führt. Um das Problem zu lösen, muss ein neues Webzertifikat erstellt werden. Siehe Ungültiges Webzertifikat und Fehler bei der Geräteregistrierung nach der Installation der IGEL UMS 12 unter Linux (see page 74).

12. Wählen Sie, ob Sie im Menü **Verknüpfungen** für UMS Konsole und UMS Administrator anlegen möchten.

13. Prüfen Sie die Zusammenfassung der Installationseinstellungen und starten Sie den Vorgang mit **Start installation**.

    ⓘ Während des Upgrades der UMS, z. B. von der Version 6.09 auf 6.10 oder von der Version 6.x auf 12.x, wird das Datenbankschema durch den Installer geändert. Bei großen Produktionsdatenbanken kann dieser Prozess bis zu 2 Stunden dauern. Brechen Sie die Installation während dieser Zeit nicht ab.

14. Wenn der Installationsvorgang zu Ende ist, öffnen Sie die UMS Konsole über das Menü oder mit dem Befehl `/opt/IGEL/RemoteManager/RemoteManager.sh`

    ⓘ Es wird allgemein NICHT empfohlen, den Befehl `RemoteManager.sh` als `sudo` auszuführen. Unter Red Hat Enterprise Linux 8 kann `RemoteManager.sh` nur ohne `sudo` ausgeführt werden.

15. Verbinden Sie die UMS Konsole mit dem UMS Server mithilfe der bestehenden Zugangsdaten. Um eine Verbindung mit der UMS Web App herzustellen, siehe Wie kann ich mich an der IGEL UMS Web App anmelden? (see page 786)

UMS 12 Kommunikationsports
Wenn Sie Änderungen am Netzwerk vornehmen möchten, sollten Sie die folgenden Ports und Pfade berücksichtigen:

- Für IGEL OS 12-Geräte ist TCP 8443 /device-connector/* erforderlich.
  SSL kann am Reverse Proxy / externen Load Balancer (siehe IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading) oder am UMS Server terminiert werden.
- Für den Import von IGEL OS 12 Apps vom IGEL App Portal in die UMS ist die URL https://app.igel.com/ (TCP 443) erforderlich.
- Für die UMS Web App sind TCP 8443 /webapp/* und /wums-app/* erforderlich.
- Für die UMS Konsole ist der Root erforderlich, d. h. TCP 8443 /*
- Für IGEL OS 11-Geräte sind TCP 30001 und TCP/UDP 30005 erforderlich.

Weitere Informationen zu UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).

IGEL UMS unter Windows aktualisieren

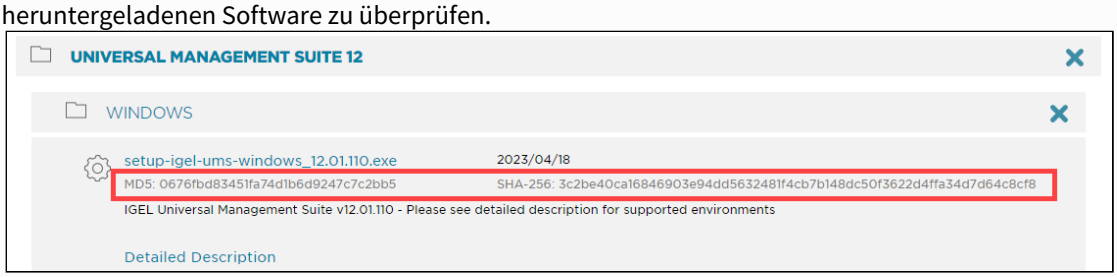
Bevor Sie ein Update der IGEL Universal Management Suite (UMS) starten, lesen Sie UMS aktualisieren (see page 298).

⚠ Erstellen Sie ein Backup der Datenbank (see page 719), bevor Sie eine zuvor installierte Version der UMS aktualisieren. Ansonsten droht Verlust aller Datenbankinhalte.

So führen Sie ein Update unter Windows aus:

1. Laden Sie die aktuelle Version der IGEL Universal Management Suite vom IGEL Downloadserver[21] herunter.

   ⓘ Aus Integritäts- und Sicherheitsgründen empfiehlt es sich, die Prüfsumme (Checksum) der heruntergeladenen Software zu überprüfen.

2. Schließen Sie andere Anwendungen und starten Sie den Installer.

   ⓘ Sie benötigen Administratorrechte, um die UMS installieren zu können.

3. Lesen und bestätigen Sie die Lizenzvereinbarung unter **License Agreement**.

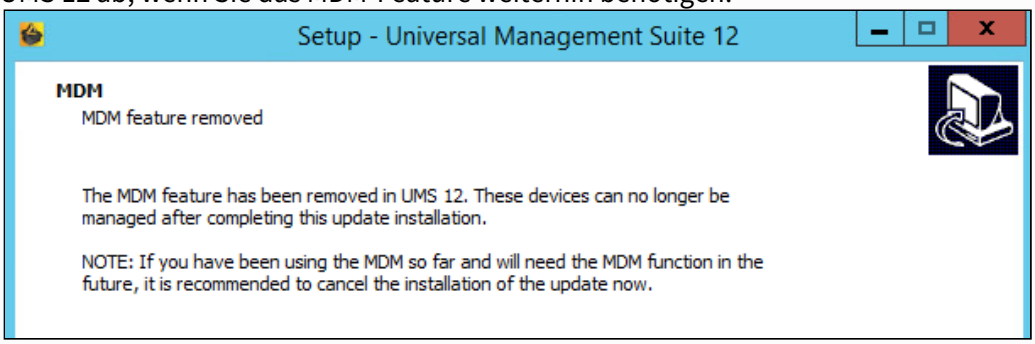
4. Lesen Sie die **Information** über den Installationsprozess und klicken Sie auf **Next**.

5. Unter **Database backup** wählen Sie den Dateinamen für die **Sicherung** der bereits existierenden Embedded-Datenbank. Wenn Sie keinen Dateinamen wählen und auf **Next** klicken, wird keine Sicherung erstellt.

   ⓘ **Nur für Update-Installationen**

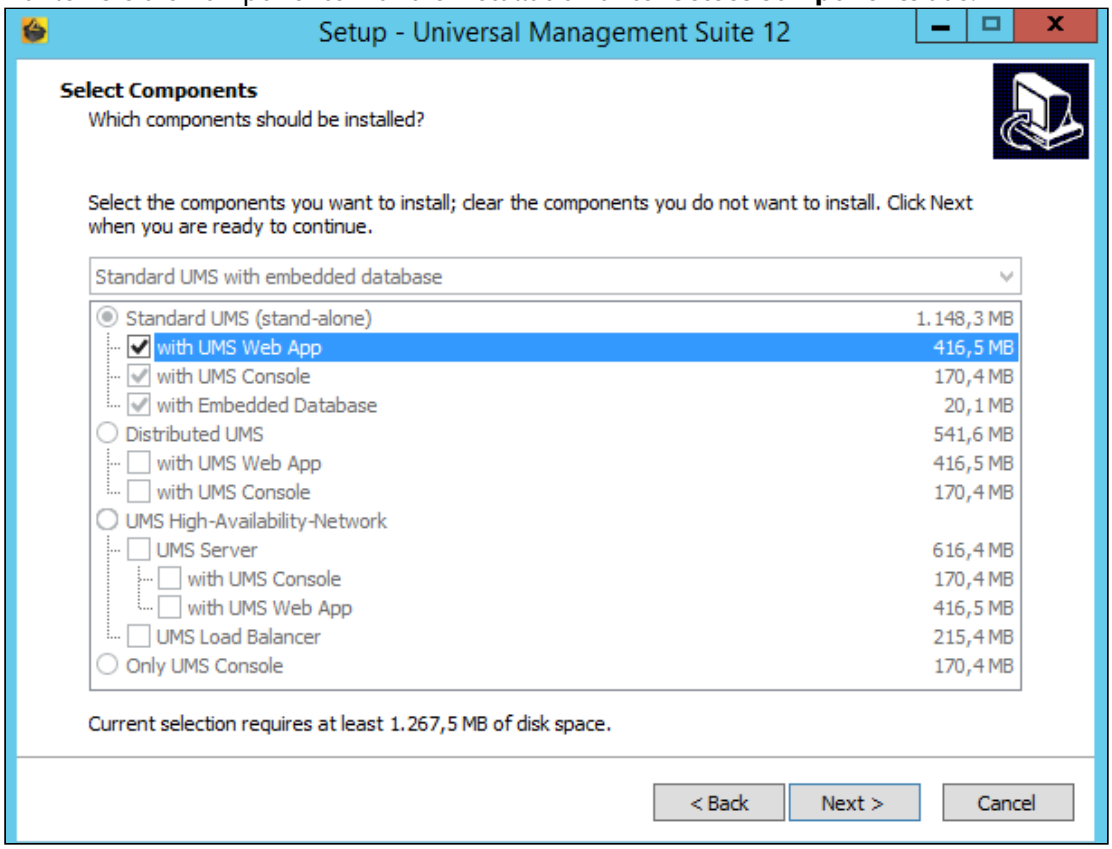
21 https://www.igel.com/software-downloads/

- Ab UMS 12 ist das MDM-Feature nicht mehr verfügbar. Brechen Sie das Upgrade auf UMS 12 ab, wenn Sie das MDM-Feature weiterhin benötigen:



- Nur wenn Sie eine Distributed UMS-Installation haben: Während der Update-Installation wird geprüft, ob nur ein UMS Server läuft und die anderen gestoppt sind. Wenn dies nicht der Fall ist, stoppen Sie alle UMS Server bis auf einen und fahren Sie mit der Aktualisierung fort; andernfalls riskieren Sie einen Datenverlust. Nachdem die Aktualisierung auf diesem Server abgeschlossen ist, können Sie die übrigen UMS Server aktualisieren, entweder parallel oder nacheinander.

6. Wählen Sie die Komponenten für die Installation unter **Select Components** aus:



- **Standard UMS**

    - **with UMS Web App**
    - **with UMS Console**
    - **with Embedded Database**
  - **Distributed UMS**
    - **with UMS Web App**
    - **with UMS Console**
  - **UMS High Availability Network**
    - **UMS Server**
      - **with UMS Web App**
    - **UMS Load Balancer**
  - **Only UMS Console**

  Informationen zu den UMS-Installationstypen finden Sie unter IGEL UMS Installation (see page 246).
  Informationen zu den Komponenten der UMS finden Sie unter Überblick über die IGEL UMS (see page 238).

7. Lesen Sie die RAM-Anforderungen unter **Memory (RAM) requirements** und klicken Sie auf **Next**, wenn Ihr System sie erfüllt.

8. Wählen Sie unter **Select Additional Tasks**, ob Sie auf dem Desktop Verknüpfungen für UMS Konsole und UMS Administrator (see page 707) anlegen möchten.

9. Wenn die interne Windows Firewall auf dem Hostrechner aktiv ist: Überprüfen Sie die Einstellungen unter **Windows firewall settings** und ändern Sie diese, falls nötig. Jeder Port, der hier aktiviert ist, wird in der Windows Firewall auf dem Hostrechner des UMS Servers als Regel definiert.

   UMS 12 Kommunikationsports
   Wenn Sie Änderungen am Netzwerk vornehmen möchten, sollten Sie die folgenden Ports und Pfade berücksichtigen:
   - Für IGEL OS 12-Geräte ist TCP 8443 /device-connector/* erforderlich.
     SSL kann am Reverse Proxy / externen Load Balancer (siehe IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading) oder am UMS Server terminiert werden.
   - Für den Import von IGEL OS 12 Apps vom IGEL App Portal in die UMS ist die URL https://app.igel.com/ (TCP 443) erforderlich.
   - Für die UMS Web App sind TCP 8443 /webapp/* und /wums-app/* erforderlich.
   - Für die UMS Konsole ist der Root erforderlich, d. h. TCP 8443 /*
   - Für IGEL OS 11-Geräte sind TCP 30001 und TCP/UDP 30005 erforderlich.

   Weitere Informationen zu UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).

10. Lesen Sie die Zusammenfassung und starten Sie den Installationsprozess.
    Der Installer installiert die neue Version der UMS, erstellt Einträge im Windows-Softwareverzeichnis sowie im Startmenü und legt, falls ausgewählt, die Verknüpfungen für die UMS Konsole und UMS Administrator auf dem Desktop ab.

> Während des Upgrades der UMS, z. B. von der Version 6.09 auf 6.10 oder von der Version 6.x auf 12.x, wird das Datenbankschema durch den Installer geändert. Bei großen Produktionsdatenbanken kann dieser Prozess bis zu 2 Stunden dauern. Brechen Sie die Installation während dieser Zeit nicht ab.

11. Nach Abschluss der Installation schließen Sie das Programm mit einem Klick auf **Finish**.
12. Starten Sie die UMS Konsole.
13. Verbinden Sie die UMS Konsole mit dem UMS Server mithilfe der bestehenden Zugangsdaten. Um eine Verbindung mit der UMS Web App herzustellen, siehe Wie kann ich mich an der IGEL UMS Web App anmelden? (see page 786)

Informationen zur unbeaufsichtigten Installation der UMS Konsole finden Sie unter Unbeaufsichtigte Installation der UMS Konsole (see page 273).

> Wenn Sie eine externe Datenbank verwenden, überprüfen Sie die Datenbankverbindung im UMS Administrator (see page 707) **>** Datenquelle (see page 729).
> Wird SQL Server AD nativ (see page 304) verwendet, müssen Sie auch den richtigen Starttyp und die richtigen Anmeldedaten für den Dienst "IGEL RMGUIServer" einstellen und den Dienst neu starten. Für Details siehe "Windows-Dienst für UMS Server konfigurieren" unter "UMS für SQL Server AD nativ einrichten" (see page 304).

Anbindung externer Datenbanksysteme

Die Verwendung eines externen Datenbanksystems wird in den folgenden Fällen empfohlen:

- Sie möchten ein großes Netzwerk von Geräten verwalten.
- In Ihrem Unternehmen ist bereits ein dediziertes Datenbanksystem im Einsatz.
- Sie verwenden die High-Availability (see page 909)- oder Distributed UMS (see page 246)-Lösung.

In anderen Fällen, eignet sich die Verwendung der Embedded-Datenbank. Sie ist in der Standardinstallation enthalten, siehe IGEL UMS unter Windows installieren (see page 266) oder IGEL UMS unter Linux installieren (see page 253).

Angaben zu den unterstützten Datenbanksystemen finden Sie in den Release Notes (see page 965) im Bereich "Supported Environment". Die Installations- und Betriebsvoraussetzungen für die Datenbank finden Sie in der Dokumentation des jeweiligen DBMS.

- Konfigurieren Sie die Datenbank im jeweiligen Verwaltungsprogramm des DBMS.
- Die Erstellung der Datenquelle und die Anbindung der UMS an die Datenbank konfigurieren Sie im UMS Administrator (see page 707) > Datenquelle (see page 729).

Achten Sie darauf, keine Sonderzeichen in Ihrem Schemanamen oder Datenbankbenutzernamen zu verwenden!

Alle UMS Server müssen mit der selben Datenbank arbeiten.

Für große High-Availability-Umgebungen werden Cluster-Datenbanken empfohlen.

Die Vorgehensweise zur Erstellung eines Backups für UMS Installationen mit der externen Datenbank finden Sie unter Ein Backup der IGEL UMS erstellen (see page 720).

Siehe auch UMS Datenbank von der Embedded-Datenbank auf Microsoft SQL Server migrieren (see page 106).

Oracle

Konfigurationshinweise

Der UMS-Server führt mehrere Dienste parallel aus, um die Funktionalität bereitzustellen. Diese Dienste stellen Verbindungen zur Datenbank her. Die Datenbank muss daher eine bestimmte Anzahl von Verbindungen zulassen. Die erwartete maximale Anzahl von Verbindungen ist
128 * [Anzahl der UMS Server]
Bitte stellen Sie sicher, dass Ihre Datenbank diese Verbindungen verarbeiten kann.

So binden Sie Oracle an:

1. Erstellen Sie in der Oracle-Datenbankverwaltung einen neuen Datenbankbenutzer mit der Rolle `Resource`.

Einige Oracle-Versionen legen die Rolle `Resource` ohne `Create View`-Berechtigung an. Stellen Sie sicher, dass diese Berechtigung in der Rolle `Resource` gesetzt ist.

Oracle

Für den ordnungsgemäßen Betrieb der UMS mit Oracle-Datenbanken, insbesondere für den Aktualisierungsvorgang, muss die Anzahl von `open_cursors` für die Datenbank angepasst werden. `open_cursors` ist eine Systemeinstellung.

1. Um den aktuellen Wert zu erfahren, melden Sie sich als `SYSDBA` an der Datenbank an und führen Sie aus:
   `SQL> select name, value from v$parameter where name = 'open_cursors';`
2. Der empfohlene Wert für `open_cursors` ist "3000". Um den Wert zu setzen, führen Sie den folgenden Befehl als `SYSDBA` aus:
   `SQL> alter system set open_cursors = 3000 scope=both;`
3. Der gleiche Befehl sollte der `SPFILE` des Oracle-Systems hinzugefügt werden, damit die Änderungen beim nächsten Neustart erhalten bleiben.

2. Legen Sie im UMS Administrator (see page 707) eine neue Datenquelle vom Typ **Oracle** an.

Oracle RAC

1. Richten Sie in der Oracle-Datenbankverwaltung einen neuen Datenbankbenutzer mit der Rolle `Resource` ein.

> Einige Oracle-Versionen legen die Rolle `Resource` ohne `Create View`-Berechtigung an. Stellen Sie sicher, dass diese Berechtigung in der Rolle `Resource` gesetzt ist.

> **Oracle**
>
> Für den ordnungsgemäßen Betrieb der UMS mit Oracle-Datenbanken, insbesondere für den Aktualisierungsvorgang, muss die Anzahl von `open_cursors` für die Datenbank angepasst werden. `open_cursors` ist eine Systemeinstellung.
>
> 1. Um den aktuellen Wert zu erfahren, melden Sie sich als `SYSDBA` an der Datenbank an und führen Sie aus:
>   `SQL> select name, value from v$parameter where name = 'open_cursors';`
> 2. Der empfohlene Wert für `open_cursors` ist "3000". Um den Wert zu setzen, führen Sie den folgenden Befehl als `SYSDBA` aus:
>   `SQL> alter system set open_cursors = 3000 scope=both;`
> 3. Der gleiche Befehl sollte der `SPFILE` des Oracle-Systems hinzugefügt werden, damit die Änderungen beim nächsten Neustart erhalten bleiben.

2. Verwenden Sie den UMS Administrator (see page 707), um für jeden Server eine neue Datenquelle vom Typ **Oracle RAC** einzurichten.

Microsoft SQL Server/Cluster with Native SQL Authentication

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

Microsoft SQL Server/Cluster with Native Active Directory (AD) Authentication

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

Microsoft SQL Server/Cluster with Active Directory (AD) Authentication via Kerberos

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

PostgreSQL

> Angaben zu den unterstützten Datenbanksystemen finden Sie in den Release Notes (see page 965) im Bereich "Supported Environment". Die Installations- und Betriebsvoraussetzungen für die Datenbank finden Sie in der Dokumentation des jeweiligen DBMS.

> **Konfigurationshinweise**
>
> Der UMS Server führt mehrere Dienste parallel aus, um die Funktionalität bereitzustellen. Diese Dienste bauen Verbindungen zur Datenbank auf. Die Datenbank muss daher eine bestimmte Anzahl von Verbindungen zulassen. Es wird empfohlen, die maximale Anzahl der Verbindungen und die Größe des gemeinsamen Puffers auf die folgenden Werte einzustellen:
>
> `max_connections = 128 * [Anzahl der UMS Server]`
>
> `shared_buffers = 128MB * [Anzahl der UMS Server]`
>
> Diese Werte werden in der Konfigurationsdatei für die PostgreSQL-Datenbank festgelegt (siehe die PostgreSQL-Dokumentation).

So binden Sie PostgreSQL an:

Setzen Sie bei der Installation einer neuen Instanz der PostgreSQL-Datenbank folgende Parameter:

- **Kodierung:** `UTF-8`
- **Adressen**: Alle Verbindungen (nicht nur `localhost`)
- **Procedural Language**: `PL/pgsql` (in der Defaultdatenbank)

Weitere Informationen zur Installation der PostgreSQL-Datenbank finden Sie unter http://www.postgresql.org[22].

Führen Sie nach der Installation folgende Konfigurationsschritte aus:

1. Stellen Sie sicher, dass in der Datei `postgresql.conf` der Parameter `listen_addresses` den Hostnamen des IGEL UMS Servers enthält oder alternativ `*` (Asterisk). Wenn `*` (Asterisk) angegeben ist, sind Verbindungen zu jedem Host zugelassen.
2. Legen Sie in der Datei `pg_hba.conf` einen Parameter `host` an, um dem UMS Server die Berechtigung für das Anmelden mit den dort definierten Benutzerdaten zu geben.

   > Wenn der IGEL UMS Server auf derselben Maschine installiert ist wie der PostgreSQL-Server, so sind keine Änderungen an diesen Dateien notwendig.
3. Starten Sie das Administrationstool pgAdmin.
4. Erstellen Sie eine neue Log-in-Rolle mit dem Namen `rmlogin.`

22 http://www.postgresql.org/

5. Erstellen Sie eine neue Datenbank mit den folgenden Parametern:
   name: `rmdb`
   owner: `rmlogin`
   encoding: `UTF-8`
6. Legen Sie ein neues Schema innerhalb der Datenbank rmdb an mit dem folgenden Parameter:
   name: `rmlogin`
7. Prüfen Sie ob die Sprache plpgsql in der Datenbank rmdb besteht.
   Falls nicht, legen Sie diese an.
8. Legen Sie im UMS Administrator (see page 707) eine neue Datenquelle an mit den folgenden Parametern:
   - **DB-Typ**: `PostgreSQL`
   - **Host**: Name des PostgreSQL-Servers
   - **Port**: Port des PostgreSQL-Servers. (Standard: 5432)
   - **Benutzer**: `rmlogin`
   - **Datenbank**: `rmdb`

Apache Derby als Datenquelle für die IGEL UMS

Der folgende Artikel erklärt, wie Sie eine externe Apache Derby Datenbank als Datenquelle für Ihre IGEL Universal Management Suite (UMS) Installation anbinden können.

> Angaben zu den unterstützten Datenbanksystemen finden Sie in den Release Notes (see page 965) im Bereich "Supported Environment". Die Installations- und Betriebsvoraussetzungen für die Datenbank finden Sie in der Dokumentation des jeweiligen DBMS.

Wir empfehlen, für die IGEL UMS eine neue Datenbankinstanz anzulegen.

Führen Sie die folgenden Schritte aus, um eine neue Datenbankinstanz in der Derby-Datenbankverwaltung anzulegen, und definieren Sie danach diese Instanz als eine Datenquelle im UMS Administrator:

1. Aktivieren Sie in der Derby-Datenbank die Option **Benutzer-Authentifizierung**.
2. Starten Sie das *ij Tool* (in `[derby-installation-dir]/bin`).
3. Führen Sie den folgenden Befehl aus, um die Datenbankinstanz `rmdb` anzulegen:
   ```
   connect 'jdbc:derby://localhost:1527/
   rmdb;user=dbm;password=dbmpw;create=true';
   ```
4. Führen Sie den folgenden Befehl aus, um das Schema `rmlogin` zu erstellen:
   ```
   create schema rmlogin;
   ```
5. Führen Sie den folgenden Befehl aus, um den UMS Datenbankbenutzer `rmlogin` mit dem Passwort `rmpassword` zu definieren:
   ```
   CALL SYSCS_UTIL.SYSCS_SET_DATABASE_PROPERTY('derby.user.rmlogin',
   'rmpassword');
   ```
6. Verlassen Sie `ij` und starten Sie den *Derby Network Server*.
7. Legen Sie im **UMS Administrator > Datenquelle** eine neue Datenquelle mit den folgenden Parametern an:
   DB-Typ: `Derby`
   Host: Name des Derby-Servers
   Port: Port des Derby-Servers. (Standard: 1527)

Benutzer: `rmlogin`

Datenbank: `rmdb`

Allgemeine Informationen zur Erstellung einer Datenquelle im UMS Administrator finden Sie unter Wie kann ich eine Datenquelle im IGEL UMS Administrator einrichten? (see page 730).

Weitere Informationen zur Installation der Derby-Datenbank finden Sie unter http://db.apache.org/derby.

Eine AWS Aurora PostgreSQL Datenbank mit der IGEL Universal Management Suite (UMS) verwenden

Dieser Artikel beschreibt, wie Sie eine Amazon Web Services (AWS) Aurora PostgreSQL-Datenbank mit der IGEL Universal Management Suite (UMS) verbinden.

> Angaben zu den unterstützten Datenbanksystemen finden Sie in den Release Notes (see page 965) im Bereich "Supported Environment". Die Installations- und Betriebsvoraussetzungen für die Datenbank finden Sie in der Dokumentation des jeweiligen DBMS.

Ihre AWS Aurora PostgreSQL Datenbank erzeugen

▶ Folgen Sie den im AWS Dokument Erstellen eines DB-Clusters und Herstellen einer Verbindung mit einer Datenbank in einem Aurora PostgreSQL-DB-Cluster[23] beschriebenen Schritten. Wichtig: Stellen Sie sicher, dass Ihre Datenbank öffentlich zugänglich ist; siehe Schritt 11, letzter Absatz.

Ihre AWS Aurora PostgreSQL Datenbank mit Ihrer UMS verbinden

▶ Erzeugen Sie im UMS Administrator (see page 707) eine neue Datenquelle mit den folgenden Parametern:

- **DB-Typ**: `PostgreSQL`
- **Host**: Fully Qualified Domain Name (FQDN) der Endpunkt-Instanz der AWS Datenbank. Dies ist der **Endpoint name** in AWS; siehe AWS Dokument[24], Abschnitt “Herstellen einer Verbindung mit einer Instance in einem Aurora PostgreSQL-DB-Cluster”, Schritt 3.
- **Port**: Port des AWS Aurora Servers (Standard: 5432)
- **Benutzer**: Benutzername, den Sie in AWS als **Master username** definiert haben; siehe AWS Dokument[25], Abschnitt "Erstellen eines Aurora PostgreSQL-DB-Clusters", Schritt 9.
- **Datenbank**: Spezifischer Datenbankname. Dies ist der **DB cluster identifier**, wie beschrieben im AWS Dokument[26], Abschnitt "Erstellen eines Aurora PostgreSQL-DB-Clusters", Schritt 8. Wenn Sie den Standardwert **DB cluster identifier** in AWS belassen haben, so belassen Sie hier den Standardwert `postgres`. Sie können den Wert in AWS unter **Additional configuration** finden.

23 https://docs.aws.amazon.com/de_de/AmazonRDS/latest/AuroraUserGuide/CHAP_GettingStartedAurora.CreatingConnecting.AuroraPostgreSQL.html
24 https://docs.aws.amazon.com/de_de/AmazonRDS/latest/AuroraUserGuide/CHAP_GettingStartedAurora.CreatingConnecting.AuroraPostgreSQL.html
25 https://docs.aws.amazon.com/de_de/AmazonRDS/latest/AuroraUserGuide/CHAP_GettingStartedAurora.CreatingConnecting.AuroraPostgreSQL.html
26 https://docs.aws.amazon.com/de_de/AmazonRDS/latest/AuroraUserGuide/CHAP_GettingStartedAurora.CreatingConnecting.AuroraPostgreSQL.html

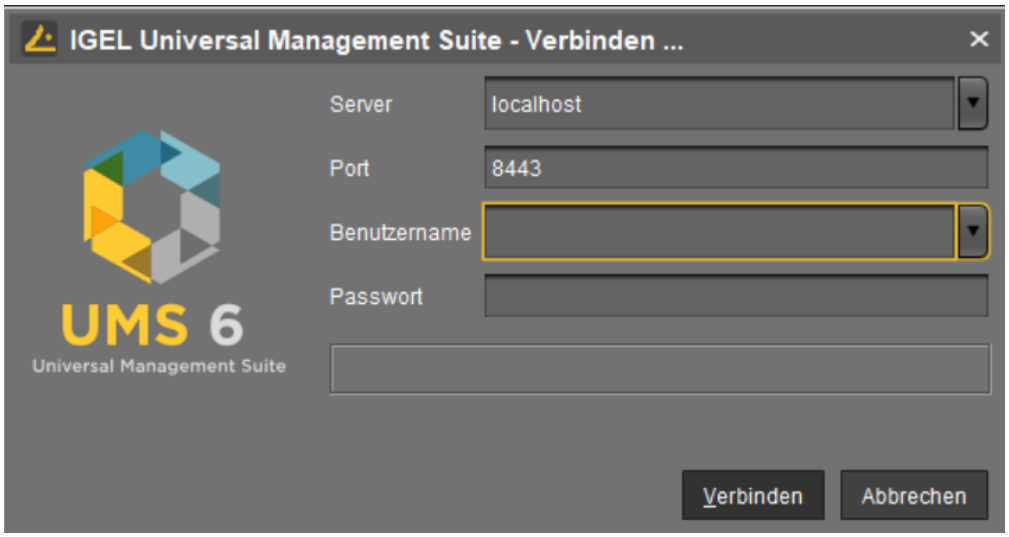
UMS Konsole mit dem IGEL UMS Server verbinden

Der folgende Artikel beschreibt, wie Sie die IGEL Universal Management Suite (UMS) Konsole mit dem UMS Server verbinden.

> Wenn Sie unter Linux die UMS Konsole vom Terminalemulator aus starten müssen, verwenden Sie den Befehl / `[IGEL Installationsverzeichnis]` / `RemoteManager.sh` (wenn das standardmäßige Installationsverzeichnis verwendet wird: `/opt/IGEL/RemoteManager/RemoteManager.sh`)
>
> Es wird allgemein NICHT empfohlen, `RemoteManager.sh` als `sudo` auszuführen. Unter Red Hat Enterprise Linux 8 kann der Befehl `RemoteManager.sh` nur ohne `sudo` ausgeführt werden.

So stellen Sie eine Verbindung zum UMS Server her:

1. Starten Sie die UMS Konsole.
2. Geben Sie die Zugangsdaten ein:
   - **Server**: Hostname oder IP-Adresse des UMS Servers. Wenn Sie sich an der lokalen UMS Konsole des Servers anmelden, geben Sie `localhost` ein oder lassen Sie das Feld leer.
   - **Port**: Port, auf dem der GUI-Server der UMS die Anfragen der UMS Konsole empfängt (Standard: 8443). Sie können den Port mit dem UMS Administrator ändern, siehe Einstellungen - Servereinstellungen im IGEL UMS Administrator ändern (see page 709).
   - **Benutzername**: Benutzername für die Verbindung zwischen UMS Konsole und Datenbank. Bei Ersteinrichtung der UMS ist das der Benutzername des Datenbank-Benutzerkontos, das während der Installation des UMS Servers erstellt wurde. Wenn Sie einer im UMS konfigurierten Domäne angehören, geben Sie `@` ein.
   - **Passwort**: Passwort für die Verbindung zwischen UMS Konsole und Datenbank. Bei Ersteinrichtung der UMS ist das das Passwort des Datenbank-Benutzerkontos, das während der Installation des UMS Servers erstellt wurde.



3. Klicken Sie **Verbinden**.

Die in **Server**, **Port** und **Benutzername** eingegebenen Daten werden für spätere Verbindungsvorgänge gespeichert. Beim nächsten Verbindungsaufbau müssen Sie lediglich das Passwort eingeben. Die zuletzt verwendeten Server- und Benutzerinformationen werden gespeichert. Sie können gespeicherten Anmeldedaten löschen unter **Extras** > **Einstellungen** > **Allgemein** > **Anmeldehistorie löschen**.

ⓘ Nach einigen fehlgeschlagenen Anmeldeversuchen über die UMS Konsole, die IMI REST API oder WebDAV (z. B. https://<server>:8443/ums_filetransfer/) werden die Benutzerkonten durch den Brute-Force-Schutz temporär für 10 Minuten gesperrt. In der UMS Konsole wird eine entsprechende Meldung angezeigt, wenn das Benutzerkonto gesperrt ist.

IGEL UMS registrieren

Für die Kommunikation Ihrer IGEL Universal Management Suite (UMS) mit den IGEL Cloud Services müssen Sie Ihre UMS registrieren.

Nur ein autorisierter Benutzer kann die UMS registrieren, siehe Verwaltung von Benutzern und Rollen im IGEL-Kundenportal. Detaillierte Anweisungen finden Sie unter Registrierung der IGEL Universal Management Suite (UMS).

Beachten Sie, dass bei einer fehlenden Registrierung der UMS folgende Fehlermeldung angezeigt wird, wenn Sie versuchen, Apps für IGEL OS 12-Geräte vom IGEL App Portal zu importieren:

```
Authentication Error
No valid token provided.
Please contact your system administrator to register your UMS.
```

IGEL OS Geräte am UMS Server registrieren

Der folgende Artikel gibt einen kurzen Überblick über mögliche Methoden für die Registrierung von Endgeräten am IGEL Universal Management Suite (UMS) Server. Je nach Anzahl der zu registrierenden Geräte, der physikalischen Verfügbarkeit der Geräte im Netzwerk usw. können Sie die Methode wählen, die Ihnen am besten passt.

Methoden zur Geräteregistrierung

> Es ist nicht erforderlich, das Gerät in der UMS zu registrieren, da dies erfolt
> - wenn Sie das Gerät mithilfe des IGEL Onboarding Service oder der Einmalpasswortmethode im IGEL Einrichtungsassistenten einbinden, siehe Onboarding IGEL OS 12 Devices (IGEL OS 12-Geräte)
> - wenn Sie die ICG-Verbindung auf dem Gerät im IGEL Setup Assistant oder im ICG Agent Setup einrichten (IGEL OS 11-Geräte)

Sie können Geräte auf folgenden Wegen am UMS Server registrieren:

- Das Netzwerk nach Geräten scannen und die gefundenen Geräte registrieren (see page 324)
  In diesem Fall müssen die Geräte physikalisch im Netz verfügbar und angeschaltet sein. Diese Methode wird in der Regel verwendet, wenn nicht so viele Geräte registriert werden müssen; für den ersten Massen-Rollout wird die automatische Registrierung von Geräten bevorzugt.

- Automatische Registrierung von Geräten (see page 337)
  Wenn Sie automatisches Registrieren aktivieren und das DHCP-Tag und/oder den DNS-Alias `igelrmserver` mit der IP oder dem FQDN des UMS Servers konfigurieren, werden alle Geräte im Netzwerk des Servers automatisch beim Start registriert.

  > IGEL empfiehlt die automatische Registrierung für die erste Registrierung neuer IGEL OS 11-Geräte beim Rollout. Sie können die automatische Registrierung auch für IGEL OS 12-Geräte benutzen, die sich innerhalb des Firmennetzwerks befinden; für IGEL OS 12-Geräte außerhalb des Firmennetzwerks wird die Verwendung von IGEL Onboarding Service bevorzugt, siehe Erstkonfiguration des IGEL Onboarding Service (OBS) und Onboarding IGEL OS 12 Devices. Deaktivieren Sie die automatische Registrierung, sobald alle Geräte registriert sind, damit kein unbekanntes Gerät sensitive Daten erhalten kann.

- Geräte importieren (see page 331)
  Hier importieren Sie die Daten der Geräte aus einer CSV-Datei, deswegen kann diese Methode nur dann verwendet werden, wenn Sie bereits genau wissen, welche Geräte zu registrieren sind. Dieser Ansatz macht es möglich, Geräte der UMS bekannt zu machen, bevor die Geräte physikalisch im Netz verfügbar sind. Bei dieser Methode können Sie auch editierbare

Geräteattribute wie Standort, Abteilung oder Kostenstelle spezifizieren.

- Geräteeintrag manuell erstellen (see page 339)
  In diesem Fall legen Sie einen Datenbankeintrag für ein Gerät manuell an. Diese Methode ist für die Ersteinrichtung der UMS nicht geeignet, da die Firmware für die Geräte bereits in der Datenbank vorhanden sein muss. Sie ist eher geeignet, um nur eine kleine Anzahl von Geräten zu registrieren.

- Funktion "UMS Registrierung" am Gerät verwenden (IGEL OS 11 und früher)
  In diesem Fall starten Sie die Funktion **UMS Registrierung** direkt auf dem Gerät und geben die Daten des gewünschten UMS Servers manuell ein.

Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube-nocookie.com/embed/1XMWDpv2wDI?autoplay=1

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube-nocookie.com/embed/_evv-Vlixwg?autoplay=1

Netzwerk nach Geräten scannen und Geräte an der IGEL UMS registrieren

Der folgende Artikel beschreibt, wie Sie Geräte an der IGEL Universal Management Suite (UMS) über die Funktion **Geräte scannen** registrieren. Diese Funktion wird sowohl für die UMS Konsole als auch für die UMS Web App beschrieben.

Einen Überblick über die Methoden für die Geräteregistrierung finden Sie unter IGEL OS Geräte am UMS Server registrieren (see page 322).

> Die Funktion für das Scannen und Registrieren von Geräten kann nur verwendet werden, wenn ein Endgerät eine direkte Verbindung zur UMS herstellen kann. Wenn also ein externer Load Balancer / Reverse Proxy konfiguriert wird, ist diese Funktion möglicherweise nicht nutzbar; siehe NGINX: Example Configuration for as Reverse Proxy in IGEL OS with SSL Offloading (see page 19).

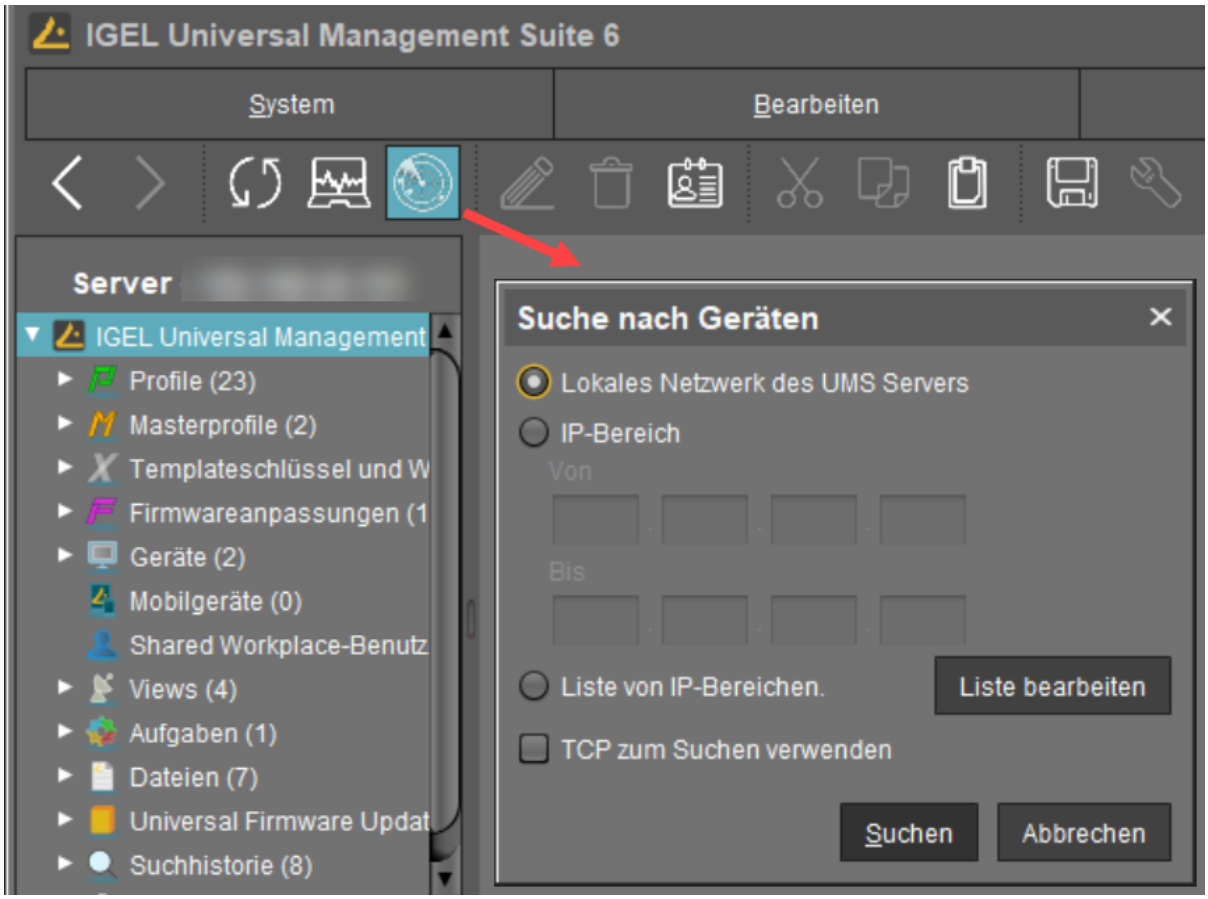
Um Geräte im Netzwerk zu finden, müssen folgende Voraussetzungen erfüllt sein:

- Die Geräte sind eingeschaltet und funktionsfähig.
- Die Firmware der Geräte unterstützt die UMS. Das ist bei folgenden Geräten der Fall:
  - IGEL Geräten mit Original-Firmware
  - Geräte, die mit IGEL OS Creator (OSC) konvetiert wurden
  - Geräte, auf denen IGEL OS über einen UD Pocket gebootet wurde
  - Geräte, auf denen IGEL OS mittels IGEL Universal Desktop Converter 3 (UDC3) installiert wurde

Scan- und Registrierungsfunktion in der UMS Konsole

So suchen Sie im Netzwerk nach Geräten und registrieren diese in der UMS:

1. Melden Sie sich an der UMS Konsole an.
2. Klicken Sie  .
   Das Fenster **Suche nach Geräten** öffnet sich.



3. Legen Sie den Suchbereich fest:
   - **Lokales Netzwerk des UMS Servers**: Der UMS Server sendet eine Broadcast-Nachricht in das Netzwerk.

     > ⓘ Bei mehreren Netzwerkschnittstellen ist zu beachten, dass die Broadcast-Nachricht nur über die erste Netzwerkschnittstelle gesendet wird. Bei Windows ist dies unter das erste Element in der Liste der Netzwerkverbindungen.

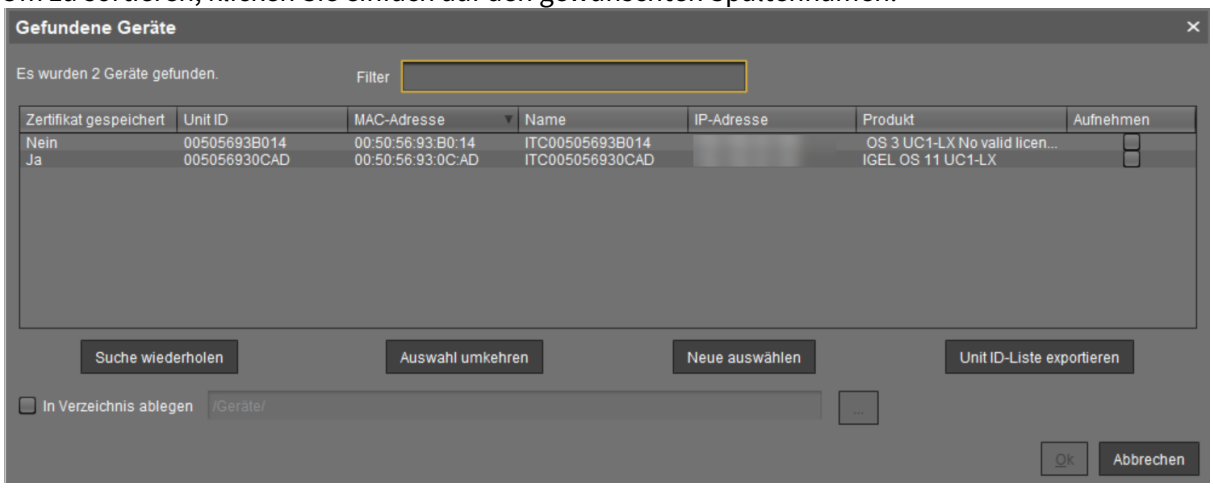
   - **IP-Bereich**: Der UMS Server kontaktiert jedes Gerät im angegebenen Bereich.
   - **Liste von IP-Bereichen**: Mit **Liste bearbeiten** können Sie die IP-Bereiche festlegen, in denen die UMS nach Geräten suchen soll.
   - **TCP zum Suchen verwenden**: Wenn die Option aktiviert ist, erfolgt die Kommunikation mit den Geräten über TCP. Wenn die Option deaktiviert ist, wird UDP verwendet.

     > ⓘ Wenn TCP zum Suchen verwendet wird, dauert der Suchvorgang länger; die Suchergebnisse können jedoch zuverlässiger sein.

4. Klicken Sie **Suchen**.
   Im Fenster **Gefundene Geräte** werden die Suchergebnisse angezeigt. Die Geräte können nun registriert werden.

Sobald Sie das Suchergebnis erhalten haben, können Sie neue Geräte registrieren:

1. Wenn Sie nur Geräte mit einem bestimmten Merkmal in einer der Spalten **Zertifikat gespeichert**, **Unit ID**, **MAC-Adresse**, **Name**, **IP-Adresse** oder **Produkt** sehen wollen, geben Sie die entsprechende Zeichenkette im Feld **Filter** ein.
   Um zu sortieren, klicken Sie einfach auf den gewünschten Spaltennamen.



> Sie können ein Gerät mit **Zertifikat gespeichert** = "Ja" nur dann registrieren, wenn die UMS das gleiche Zertifikat hat.
> "Ja" für **Zertifikat gespeichert** bedeutet, dass das Gerät bereits ein Serverzertifikat von irgendeiner UMS erhalten hat, d. h.
> - das Gerät wurde bereits an der aktuellen UMS registriert. In diesem Fall wird das Gerät einfach neu registriert, da die UMS und das Gerät das gleiche Zertifikat haben. Sie können jedoch vorab nach dem Gerät suchen, wenn Sie überprüfen wollen, ob es an dieser UMS und nicht an einer anderen UMS registriert ist, siehe Suche nach Objekten in der UMS (see page 363).
>   ODER
> - das Gerät wurde bereits an einer anderen UMS registriert. In diesem Fall siehe Troubleshooting: Die Registrierung eines Geräts über Suche nach Geräten schlägt fehl (see page 165).

2. Wählen Sie die Geräte aus, die registriert werden sollen. Sie haben folgende Möglichkeiten:
   - Manuelle Auswahl: Markieren Sie in der Spalte **Aufnehmen** die zu registrierenden Geräte.
   - Auswahl aller noch nicht registrierten Geräte: Klicken Sie auf **Neue auswählen**. Damit werden alle Geräte markiert, die noch kein Serverzertifikat von der UMS erhalten haben.

3. Klicken Sie **OK**.
   Die Geräte werden in der UMS Datenbank registriert. Dies kann einige Zeit dauern.

   > Bei der Registrierung wird das Serverzertifikat der UMS auf dem Gerät gespeichert. Der weitere Zugriff auf das Gerät wird nach diesem Zertifikat validiert. Nur der Eigentümer des Zertifikats kann das Gerät verwalten.

   Das Ergebnis des Vorgangs und mögliche Fehlermeldungen werden in einem neuen Fenster angezeigt.

   Die Geräte werden im Verzeichnis **Geräte** des Strukturbaums abgelegt, falls kein anderes Verzeichnis unter **In Verzeichnis ablegen** angegeben wurde.

Scan- und Registrierungsfunktion in der UMS Web App

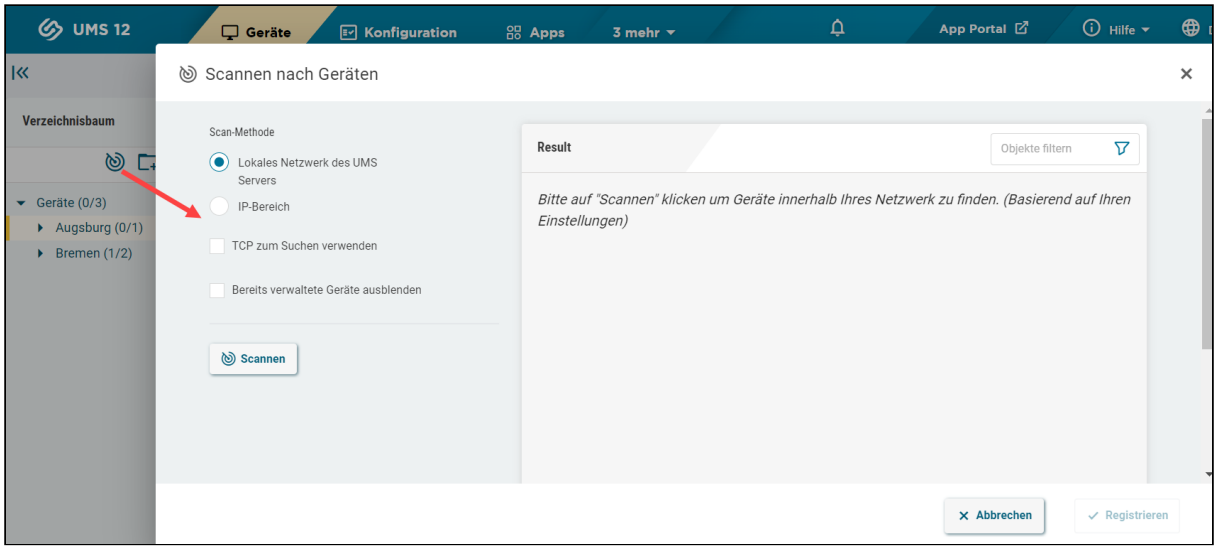
So suchen Sie im Netzwerk nach Geräten und registrieren diese in der UMS:

1. Öffnen Sie die UMS Web App und gehen Sie zu **Geräte**.

2. Wenn Sie möchten, dass die Geräte bei der Registrierung in einem bestimmten Verzeichnis abgelegt werden, markieren Sie das gewünschte Verzeichnis im Strukturbaum. Wenn kein bestimmtes Verzeichnis ausgewählt ist, werden die Geräte im Verzeichnis **Geräte** abgelegt.

3. Klicken Sie **Suche nach Geräten** .

   Das Fenster **Scannen nach Geräten** öffnet sich.



4. Legen Sie den Suchbereich fest:

- **Lokales Netzwerk des UMS Servers**: Der UMS Server sendet eine Broadcast-Nachricht in das Netzwerk.

  > Bei mehreren Netzwerkschnittstellen ist zu beachten, dass die Broadcast-Nachricht nur über die erste Netzwerkschnittstelle gesendet wird. Bei Windows ist dies unter das erste Element in der Liste der Netzwerkverbindungen.

- **IP-Bereich**: Der UMS Server kontaktiert jedes Gerät im angegebenen Bereich. Um den IP-Bereich anzugeben, verwenden Sie das Format [IP-Start] - [IP-End], z. B. `192.168.0.0 - 192.168.178.210`. Um mehrere IP-Bereiche anzugeben, drücken Sie `[Enter]`.

- **TCP zum Suchen verwenden**: Wenn die Option aktiviert ist, erfolgt die Kommunikation mit den Geräten über TCP. Wenn die Option deaktiviert ist, wird UDP verwendet.

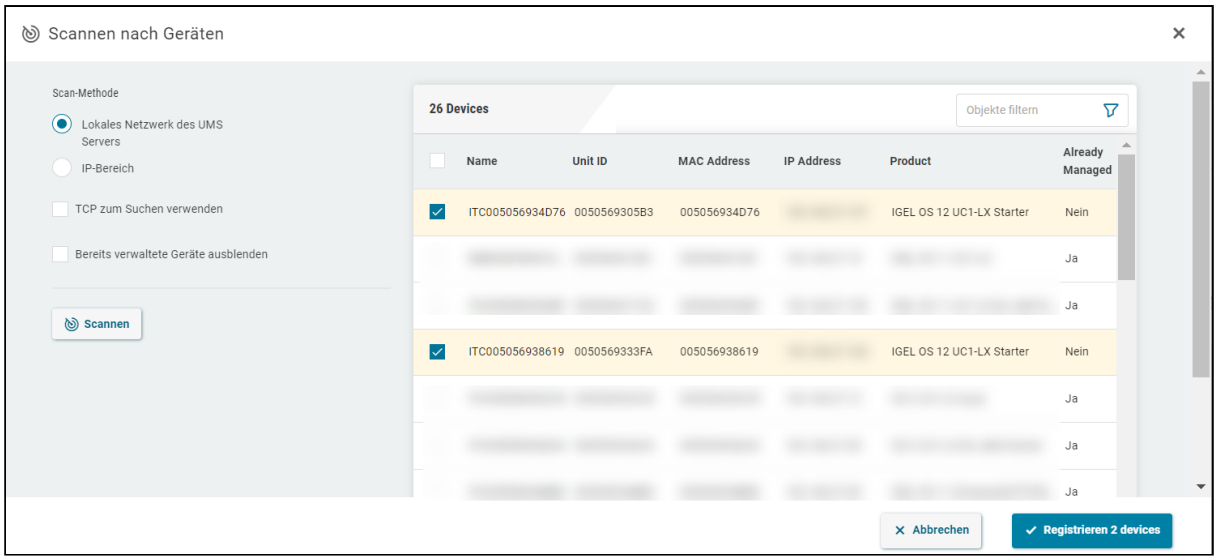
  > Wenn TCP zum Suchen verwendet wird, dauert der Suchvorgang länger; die Suchergebnisse können jedoch zuverlässiger sein.

- **Bereits verwaltete Geräte ausblenden**: Geräte, die bereits registriert wurden, d. h. die ein Serverzertifikat von einer UMS bereits haben, werden in den Suchergebnissen nicht angezeigt.

5. Klicken Sie **Scannen**.
   Die Suchergebnisse werden angezeigt. Die Geräte können nun registriert werden.

Sobald Sie das Suchergebnis erhalten haben, können Sie neue Geräte registrieren:

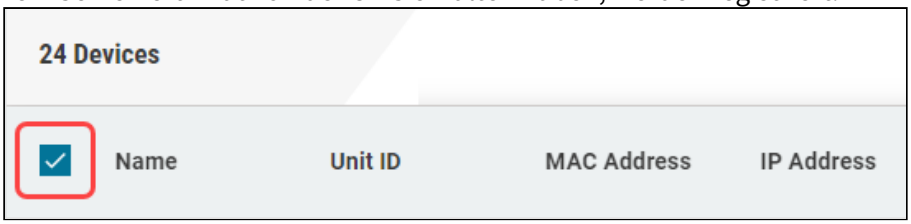
1. Wenn Sie nur Geräte mit einem bestimmten Merkmal in einer der Spalten **Name**, **Unit ID**, **MAC-Adresse**, **IP-Adresse** oder **Produkt** sehen wollen, geben Sie die entsprechende Zeichenkette im Feld **Objekte filtern** ein.
   Um die Ergebnisse in der Spalte **Already Managed** zu filtern, aktivieren oder deaktivieren Sie **Bereits verwaltetete Geräte ausblenden**.



Ein Gerät mit **Already Managed** = "Ja" wird nur dann registriert, wenn die UMS das gleiche Zertifikat hat.
"Ja" für **Already Managed** bedeutet, dass das Gerät bereits ein Serverzertifikat von irgendeiner UMS erhalten hat, d. h.

- das Gerät wurde bereits an der aktuellen UMS registriert. In diesem Fall wird das Gerät einfach neu registriert, da die UMS und das Gerät das gleiche Zertifikat haben. Sie können jedoch vorab nach dem Gerät suchen oder den Papierkorb (see page 545) überprüfen, wenn Sie sicherstellen wollen, ob es an dieser UMS und nicht an einer anderen UMS registriert ist, siehe Suche nach Objekten in der UMS (see page 363).
  ODER
- das Gerät wurde bereits an einer anderen UMS registriert. In diesem Fall siehe Troubleshooting: Die Registrierung eines Geräts über Suche nach Geräten schlägt fehl (see page 165).

2. Wählen Sie die Geräte aus, die registriert werden sollen. Sie haben folgende Möglichkeiten:
   - Manuelle Auswahl: Wählen Sie die zu registrierenden Geräte einzeln aus.
   - Auswahl aller Geräte: Dadurch werden alle Geräte markiert, aber nur die Geräte, die noch kein Serverzertifikat von der UMS erhalten haben, werden registriert:



3. Prüfen Sie, ob unter **Geräte zum Verzeichnis hinzufügen** das richtige Verzeichnis ausgewählt ist.

4. Klicken Sie **Registrieren**.
   Die Geräte werden in der UMS Datenbank registriert. Dies kann einige Zeit dauern.

   > Bei der Registrierung wird das Serverzertifikat der UMS auf dem Gerät gespeichert. Der weitere Zugriff auf das Gerät wird nach diesem Zertifikat validiert. Nur der Eigentümer des Zertifikats kann das Gerät verwalten.

Geräte importieren

Sie können Geräte der UMS bekannt machen, bevor die Geräte physikalisch im Netz verfügbar sind. Damit können Sie editierbare Attribute wie beispielsweise Abteilung oder Kostenstelle festlegen. Hierzu importieren Sie die Daten der Geräte aus einer CSV-Datei.

> Für eine vollständige Registrierung von Geräten müssen die Firmwaredaten der Geräte in der UMS vorhanden sein. Weitere Informationen finden Sie unter Firmwares importieren (see page 469).

So importieren Sie Geräte:

1. Konfigurieren Sie Ihren DHCP- und DNS-Server wie unter Geräte automatisch an der IGEL UMS registrieren (see page 337), Schritt 2 beschrieben.
2. Wählen Sie **System** > **Importieren** > **Geräte importieren**.
3. Klicken Sie **Datei öffnen** und wählen Sie die Datei aus.
4. Wählen Sie das zutreffende Format, d. h. das Format, in dem die Daten vorliegen:
   - **Kurzes Format**: Siehe Import mit kurzem Format (see page 332)
   - **Langes Format**: Siehe Import mit langem Format (see page 333)
   - **IGEL Seriennummern Format**: Siehe Import mit IGEL Seriennummer (see page 335)
5. Wenn Einträge als fehlerhaft markiert sind, klicken Sie auf **Bereinigen**, um alle Meldungen aus der Anzeige zu löschen.
6. Klicken Sie **Geräte importieren**, um den Importvorgang zu starten.

So korrigieren Sie fehlerhafte Enträge:

▶ Ändern Sie die rot markierten Einträge mit den folgenden Bearbeitungsfunktionen:

- [Strg-C] und [Strg-V] zum Kopieren und Einfügen einer markierten Zeile
- [Entf/Strg-X] zum Löschen einer markierten Zeile
- [Return/Eingabe] fügt eine weitere Zeile unter einem Feld hinzu.

Import mit kurzem Format

Das kurze Format liefert die für den Import notwendigen Informationen und die Zuordnung zu einem Profil. Die Importdatei sollte in UTF-8 kodiert sein.

- **Unit ID**: Wenn das Gerät ein IGEL Gerät oder ein mit UDC3 oder IGEL OS Creator (OSC) konvertiertes Gerät ist, so ist die Unit ID identisch mit der MAC-Adresse des Geräts. Wenn das Gerät ein UD Pocket ist, so ist die Unit ID im USB-Stick des UD Pocket fest verdrahtet.
- **Name**: Gerätename

  - Die maximale Länge des Gerätenamens ist auf 15 Zeichen begrenzt, wenn **Netzwerknamen anpassen, falls UMS-interner Name geändert wurde** unter UMS-Konsole > **UMS Administration > Globale Konfiguration > Geräte-Netzwerkeinstellungen** aktiviert ist.
  - Die Länge des Gerätenamens ist nicht begrenzt, wenn **Netzwerknamen anpassen, falls UMS-interner Name geändert wurde** und **Namenskonvention** unter **UMS Administration > Globale Konfiguration > Geräte-Netzwerkeinstellungen** nicht aktiviert sind.
  - Jeder Gerätename wird automatisch gemäß der Namenskonvention überschrieben, auch wenn **Netzwerknamen anpassen, falls UMS-interner Name geändert wurde** aktiviert ist, falls **Namenskonvention aktivieren** unter **UMS Administration > Globale Konfiguration > Geräte-Netzwerkeinstellungen** ausgewählt ist.

  Siehe auch Thin Client Network Settings (see page 332).
- **Firmware-ID**: ID der auf dem Gerät installierten Firmware.

  Die ID einer bereits registrierten Firmware finden Sie über **Extras** > **Firmwarestatistik**.
- **Profilzuordnungen**: ID des zugeordneten Profils oder kommaseparierte Liste von IDs, falls dem Gerät mehrere Profile zugeordnet werden sollen.

  Sie können eine bereits vorhandene Profilzuordnung entfernen, indem Sie der Profil-ID ein Ausrufezeichen voranstellen. Beispiel: `!12`

  Die ID eines Profils wird in den **Beschreibungsdaten** und im **Tooltip** des Profils angezeigt.

Code-Beispiel

```
00E0C5540B8B;IGEL-Office15-2;111;26
00E0C5540B8C;IGEL-Office15-3;111;12,26,27
00E0C5540B8D;IGEL-Office16-1;111;12
```

Import mit langem Format

Das lange Format stellt ausführliche Daten bereit, wie im Folgenden beschrieben. Die Importdatei sollte UTF-8-kodiert sein.

- **Verzeichnis**: Ablageverzeichnis im Strukturbaum der UMS
- **Unit ID**: Wenn das Gerät ein IGEL Gerät oder ein mit UDC3 oder IGEL OS Creator (OSC) konvertiertes Gerät ist, so ist die Unit ID identisch mit der MAC-Adresse des Geräts. Wenn das Gerät ein UD Pocket ist, so ist die Unit ID im USB-Stick des UD Pocket fest verdrahtet.
- **Produkt und Version**: Produktname und Firmwareversion des Geräts (durch Semikolon getrennt)
- **Name**: Gerätename

  - Die maximale Länge des Gerätenamens ist auf 15 Zeichen begrenzt, wenn **Netzwerknamen anpassen, falls UMS-interner Name geändert wurde** unter UMS-Konsole > **UMS Administration > Globale Konfiguration > Geräte-Netzwerkeinstellungen** aktiviert ist.
  - Die Länge des Gerätenamens ist nicht begrenzt, wenn **Netzwerknamen anpassen, falls UMS-interner Name geändert wurde** und **Namenskonvention** unter **UMS Administration > Globale Konfiguration > Geräte-Netzwerkeinstellungen** nicht aktiviert sind.
  - Jeder Gerätename wird automatisch gemäß der Namenskonvention überschrieben, auch wenn **Netzwerknamen anpassen, falls UMS-interner Name geändert wurde** aktiviert ist, falls **Namenskonvention aktivieren** unter **UMS Administration > Globale Konfiguration > Geräte-Netzwerkeinstellungen** ausgewählt ist.

  Siehe auch Thin Client Network Settings (see page 333).
- **Standort**: Standort des Geräts
- **Abteilung**: Abteilung, der das Gerät zugeordnet ist
- **Kommentar**: Kommentar zum Gerät
- **Inventarnummer**: Inventarnummer des Geräts
- **Inbetriebnahme**: Datum, an dem das Gerät in Betrieb genommen wurde
- **Seriennummer**: Seriennummer des Geräts
- **Profilzuordnung**: ID des zugeordneten Profils oder Liste von durch Kommas getrennten IDs, falls dem Gerät mehrere Profile zugeordnet werden sollen

  Sie können eine bereits vorhandene Profilzuordnung entfernen, indem Sie der Profil-ID ein Ausrufezeichen voranstellen. Beispiel: `!12`

  Die ID eines Profils wird in den Beschreibungsdaten und im Tooltip des Profils angezeigt.
- **Kostenstelle**: Kostenstelle, der das Gerät zugeordnet ist

Code-Beispiel

```
/Import;00E0C5540B9A;IGEL OS 11;11.01.100.01;IGEL-1;Büro1;EDV;Meier;0815;01.06.2019;F44M;26;01
/Import;00E0C5540B9B;IGEL OS 11;11.01.100.01;IGEL-2;Büro2;EDV;Müller;4711;01.06.2019;F45M;26;01
/Import;00E0C5540B9C;IGEL OS 11;11.01.100.01;IGEL-2;Büro3;EDV;Schulz;42;01.06.2019;F46M;26;01
```

Der Schrägstrich "/" bedeutet, dass die Geräte im Stammverzeichnis abgelegt werden. In den obigen Beispielen werden die Geräte somit in den Ordner "Import" unter dem Wurzelverzeichnis abgelegt (der Ordner "Import" muss existieren).

Import mit IGEL Seriennummer

Sie können bei der Bestellung Ihrer IGEL Geräte eine Importdatei im Seriennummernformat anfordern. Alternativ können Sie Ihre eigene Importdatei erstellen und dabei ein alternatives Format verwenden. Beide Formate sind CSV-basiert.

> Diese Methode funktioniert nur für IGEL UD-Geräte.

Sowohl das Format einer von IGEL gesendeten Importdatei als auch das alternative Format legen die Felder **Seriennummer** und **MAC-Adresse** fest.

Von IGEL gesendetes Seriennummernformat

In einer von IGEL gesendeten Importdatei besteht das Seriennummernformat aus 5 Feldern. Hierbei werden nur die **Seriennummer** (zweites Feld) und die **MAC-Adresse** (drittes Feld) in der Datei festgelegt.

Beispiel:

```
;14D3F5002B290902DD ;00E0C521B4E4 ; ;
;14D3F5002B29090441 ;00E0C521B648 ; ;
;14D3F5002B2909056F ;00E0C521B776 ; ;
;14D3F5002B29090648 ;00E0C521B84F ; ;
;14D3F5002B2909070B ;00E0C521B912 ; ;
```

Alternatives Seriennummernformat

Das alternative Format hat 2 Felder. Die Reihenfolge der Felder ist beliebig.

Beispiel:

Sequenz MAC-Adresse - Seriennummer:

```
00E0C51B37F8;14D3D3C03B174120D0
```

Sequenz Seriennummer - MAC-Adresse:

```
14D3D3C03B174120D0;00E0C51B37F8
```

Importfelder

Bei beiden Importformaten füllt die UMS die Felder **Name** und **Version** selbst aus. Im Folgenden sind alle für importierte Geräte vordefinierten Felder beschrieben.

MAC-Adresse: MAC-Adresse des Geräts.

Name: Gerätename.

> Die maximale Länge des Gerätenamens ist auf 15 Zeichen begrenzt, wenn **Netzwerknamen anpassen, falls UMS-interner Name geändert wurde** unter UMS-Konsole > **UMS Administration > Globale Konfiguration > Geräte-Netzwerkeinstellungen** aktiviert ist.

Die Länge des Gerätenamens ist nicht begrenzt, wenn **Netzwerknamen anpassen, falls UMS-interner Name geändert wurde** und **Namenskonvention** unter **UMS Administration > Globale Konfiguration > Geräte-Netzwerkeinstellungen** nicht aktiviert sind.
Jeder Gerätename wird automatisch gemäß der Namenskonvention überschrieben, auch wenn **Netzwerknamen anpassen, falls UMS-interner Name geändert wurde** aktiviert ist, falls **Namenskonvention aktivieren** unter **UMS Administration > Globale Konfiguration > Geräte-Netzwerkeinstellungen** ausgewählt ist.
Siehe auch Thin Client Network Settings (see page 335).

Version: Firmwareversion des Geräts; wird durch die UMS zugewiesen. Die Firmware mit der höchsten ID wird dem Gerät zugewiesen. Die IDs der bereits registrierten Firmwareversionen sind unter **Extras > Firmwarestatistik** zu finden.

Seriennummer: Seriennummer des Geräts.

Geräte automatisch an der IGEL UMS registrieren

Im folgenden Artikel erfahren Sie, wie Sie die automatische Registrierung von Endgeräten an der IGEL Universal Management Suite (UMS) konfigurieren. Weitere Informationen zur Automatisierung des Rollouts mit Zero Touch Deployment finden Sie unter Roll-out-Prozess in der IGEL UMS automatisieren (see page 83).

Einen allgemeinen Überblick über die Methoden für die Geräteregistrierung finden Sie unter IGEL OS Geräte am UMS Server registrieren (see page 322).

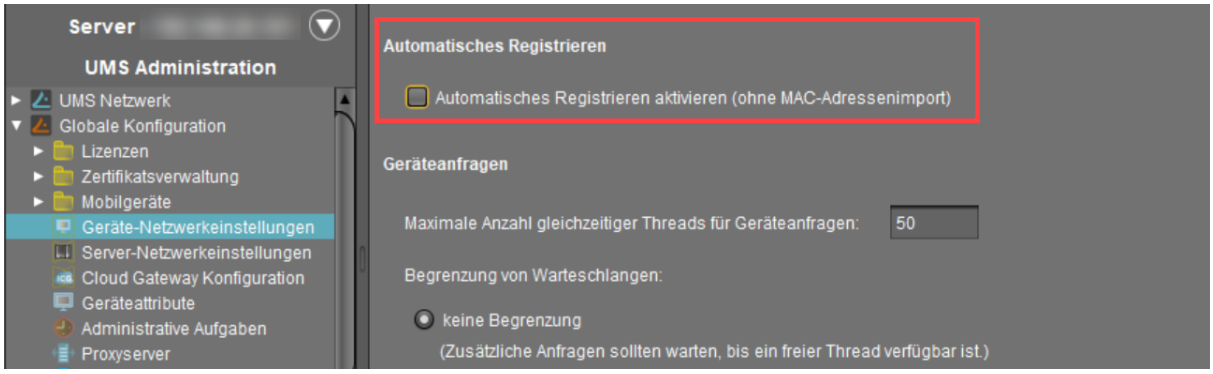
Sie können den UMS Server so konfigurieren, dass alle IGEL OS-Geräte im Netzwerk des Servers automatisch beim Start registriert werden. Hierfür muss den Geräten per **DHCP oder DNS** die Adresse des UMS Servers mitgeteilt werden.

> IGEL empfiehlt die automatische Registrierung für die erste Registrierung neuer IGEL OS 11-Geräte beim Rollout. Sie können die automatische Registrierung auch für IGEL OS 12-Geräte benutzen, die sich innerhalb des Firmennetzwerks befinden; für IGEL OS 12-Geräte außerhalb des Firmennetzwerks wird die Verwendung von IGEL Onboarding Service bevorzugt, siehe Erstkonfiguration des IGEL Onboarding Service (OBS) und Onboarding IGEL OS 12 Devices.
> Deaktivieren Sie die automatische Registrierung, sobald alle Geräte registriert sind, damit kein unbekanntes Gerät sensitive Daten erhalten kann.

So konfigurieren Sie UMS Server und Geräte für die automatische Registrierung:

1. Aktivieren Sie unter **UMS Administration** > **Globale Konfiguration** > **Geräte-Netzwerkeinstellungen** das Kontrollkästchen **Automatisches Registrieren aktivieren (ohne MAC-Adressenimport)**.

   > Ist diese Option aktiviert, wird jedes Gerät ohne UMS-Zertifikat (wird bei einer Registrierung auf den Clients verteilt) im Netzwerk in die UMS Datenbank aufgenommen. Wenn Sie ein Gerät auf die Werkseinstellungen zurücksetzen und neu starten, wird er sofort erneut auf dem Server registriert.



2. Konfigurieren Sie die Netzwerkumgebung für eine automatische UMS-Registrierung:

- **Per DNS**:
  Legen Sie auf Ihrem DNS-Server einen DNS-Eintrag `igelrmserver` (Eintragstyp A) an, der auf den UMS Server verweist.
- **Per DHCP**:
  Ändern Sie die DHCP-Serverkonfiguration je nach der IGEL OS-Version Ihrer Endgeräte wie folgt:
  - **IGEL OS 11.03.500 oder niedriger**: Setzen Sie `igelrmserver` als DHCP-Option 224. Legen Sie die DHCP-Option 224 als Zeichenfolge - nicht als DWORD - auf die IP-Adresse des Servers fest. Für den Standard-Linux-DHCP-Server fügen Sie in der Datei `dhcpd.conf` im entsprechenden Abschnitt, z.B. im globalen Bereich, Folgendes hinzu: `option igelrmserver code 224 = text` `option igelrmserver ""`
  - **IGEL OS 11.04.100 oder höher**: Alternativ können Sie die DHCP-Option 43 (vendor-specific options) verwenden, um die DHCP-Option 224 (Name: `igelrmserver`) an die richtigen Endgeräte zu senden. Ein Endgerät mit IGEL OS 11.04.100 oder höher sendet die Option 60 (vendor class identifier) mit `igel-dhcp-1` als Wert.

    > Eine IGEL-spezifische DHCP-Option, die in DHCP-Option 43 gesendet wird, überschreibt eine entsprechende DHCP-Option, die im globalen Namensraum gesendet wird. Die DHCP-Optionen 1, 224 und 226 können in Option 43 eingebettet werden.
    > Sie können verhindern, dass eine DHCP-Option 224, die im globalen Namensraum gesendet wurde, interpretiert wird. Um dies zu erreichen, müssen Sie Option 1 (Name "exklusiv", Typ Byte, Wert 1) zur DHCP-Option 43 hinzufügen.

Geräte manuell erstellen

Sie können die Datensätze für Geräte manuell erstellen.

> Die Firmware der Geräte muss bereits in der Datenbank vorhanden sein, entweder durch eine bereits erfolgte Registrierung der Geräte oder durch Import der Firmware. Daher eignet sich diese Methode nur bedingt für die Ersteinrichtung der UMS.

So erzeugen Sie manuell einen Eintrag eines Gerätes direkt in der Datenbank:

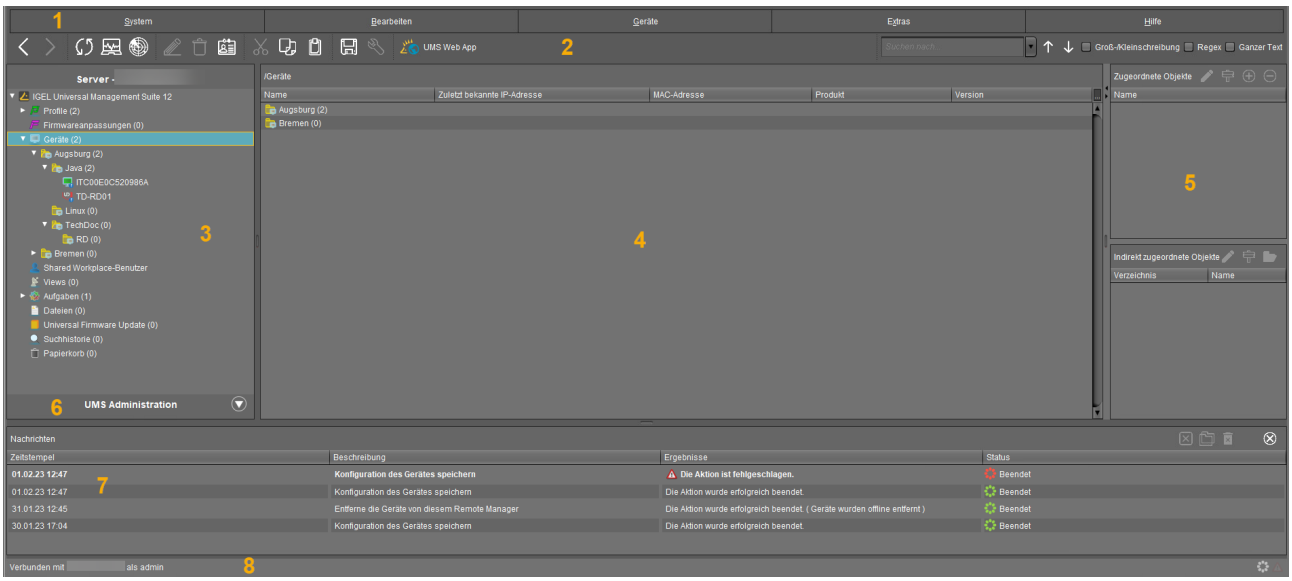
1. Wählen Sie im Kontextmenü eines Geräteverzeichnisses die Option **Neues Gerät**.
2. Geben Sie die **MAC-Adresse**, den **Namen** und die **Firmware** des Geräts an und wählen Sie optional ein **Verzeichnis** für das Gerät.
3. Geben Sie die folgenden Daten ein:
   - **MAC-Adresse**: MAC-Adresse des Geräts
   - **Version**: Firmwareversion des Geräts
   - **Name**: Gerätename
   - **Verzeichnis** (optional): Verzeichnis, in dem das Gerät angezeigt werden soll

Benutzeroberfläche der UMS Konsole

Im Folgenden werden die Bedienoberfläche der Komponenten *UMS* Konsole sowie *UMS* Administrator beschrieben.

Das Konsolenfenster

Die UMS Konsole enthält die folgenden Bereiche:



1	Menüleiste	Alle Befehle und Aktionen können aus dem Menü heraus gestartet werden. Sie können Shortcuts ([Alt] + unterstrichenes Zeichen des Menüelements) verwenden, um über die Tastatur auf die Menüleiste zuzugreifen. Siehe Menüleiste der IGEL UMS Konsole (see page 343).
2	Symbolleiste	Häufig verwendete Befehle, die Objekte im Strukturbaum betreffen. Siehe Symbolleiste (see page 355).
3	Strukturbaum	Zugriff auf alle UMS Objekte wie am UMS Server registrierte Geräte, Verzeichnisse, Profile, Views, geplante Aufgaben usw. Siehe Strukturbaum der IGEL UMS Konsole (see page 354).
4	Inhaltsbereich	Informationen zum ausgewählten Objekt. Viele Eingabefelder können direkt bearbeitet werden. Siehe Inhaltsbereich der IGEL UMS Konsole (see page 357).
5	Zugeordnete Objekte	Objekte, die den Geräten oder Ordnern zugeordnet sind. Siehe Zugeordnete Objekte (see page 361).

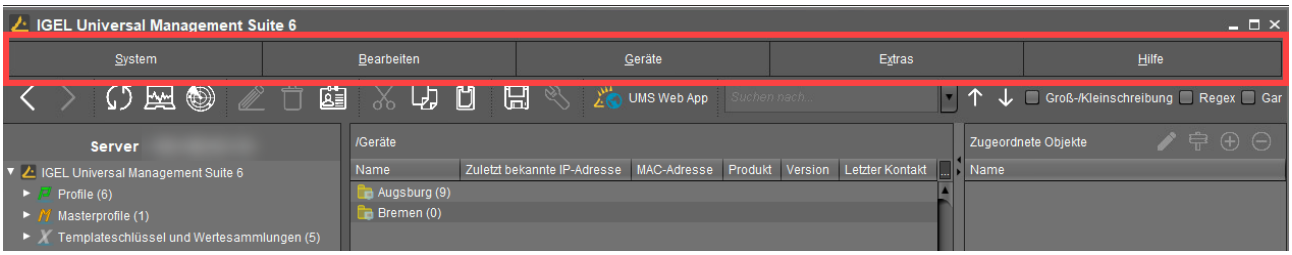
6	UMS Administration	Verwaltungsaufgaben wie z. B. die Konfiguration der Domänen, Universal Firmware Updates und das zeitgesteuerte Backup der UMS Datenbank (nur Embedded-DB) Siehe UMS Administration (see page 549).
7	Nachrichten	Meldungen zu Aktionen, die in der UMS Konsole gestartet werden. Meldungen zu erfolgreichen Vorgängen werden in grüner Farbe angezeigt. Meldungen zu Problemen bei der Ausführung werden in roter Farbe angezeigt. Siehe Nachrichten (see page 359).
8	Statuszeile	Statusmeldungen der Konsole wie z. B. der aktuell verbundene Server und der Benutzername. Siehe Statuszeile (see page 360).

Sie können die vertikalen und horizontalen Begrenzungen zwischen Strukturbaum/UMS Administration, Inhaltsbereich und Nachrichten verändern, um die Abmessungen der Bereiche ihren Bedürfnissen anzupassen. Ab UMS Version 5.02.100 werden die Änderungen gespeichert, so dass sie bei der nächsten Anmeldung wieder zur Verfügung stehen.

Menüleiste der IGEL UMS Konsole

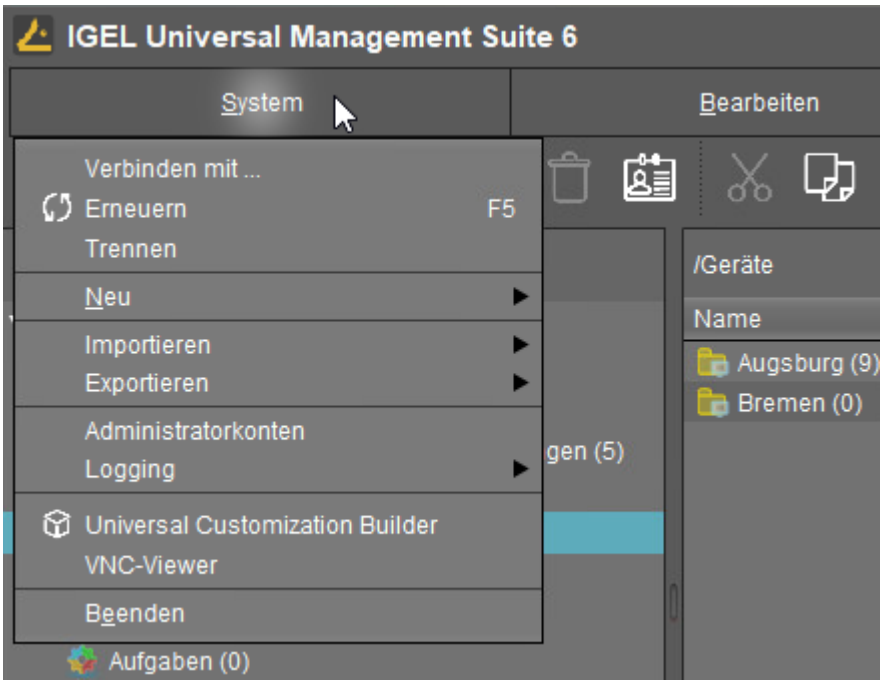
Im folgenden Artikel lernen Sie über die Einstellungen, die Sie in der Menüleiste der IGEL Universal Management Suite (UMS) Konsole vornehmen können.

Die Menüleiste der UMS Konsole besteht aus den folgenden Menüs:



System

In diesem Menü finden Sie Optionen für Aktionen rund um die UMS:



Verbinden mit: Verbindung zum UMS Server herstellen; die bestehende Verbindung wird geschlossen und die neue Verbindung wird im gleichen UMS Konsolenfenster angezeigt. Detaillierte Informationen finden Sie unter UMS Konsole mit dem IGEL UMS Server verbinden (see page 319).

- **Server**: IP oder Hostnamen des UMS Servers

- **Port**: Portnummer, Standard: 8443
- **Benutzername**: Benutzername, bei LDAP-Benutzern '@'
- **Passwort**: Benutzerpasswort

Erneuern: Ansicht aktualisieren.

Trennen: Verbindung zum UMS Server trennen.

Neu: Neue UMS Objekte wie Verzeichnis, Profil, Aufgabe, usw. anlegen

Importieren: Objekte wie Firmware, Profil, Gerät importieren. Detaillierte Informationen finden Sie unter Daten exportieren und importieren (see page 467), Profile exportieren und importieren (see page 390) und Geräte importieren (see page 331).

Exportieren: Objekte wie Firmware, Profil, Gerät exportieren

Administratorkonten: UMS Benutzerkonten und Benutzergruppen anlegen und verwalten. Detaillierte Informationen finden Sie unter Administratorkonten und Zugriffsrechte (see page 676).

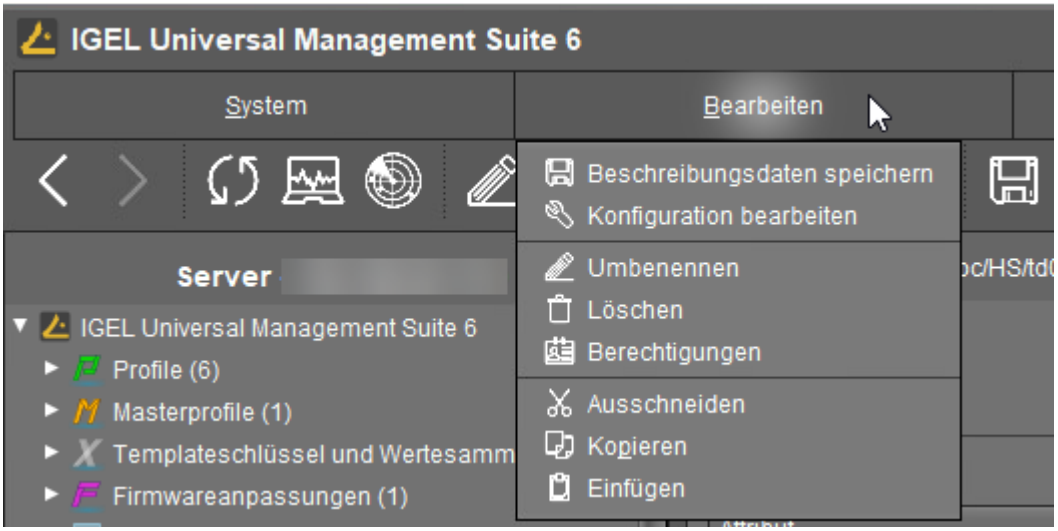
Logging: Anzeige und Export der Aufzeichnungen von Nachrichten, Ereignissen und VNC-Log-Einträgen. Detaillierte Informationen finden Sie unter Logging (see page 661) und Benutzeraktionen protokollieren (see page 694).

VNC-Viewer: Ein Gerät spiegeln. Details zu Spiegeln finden Sie unter Spiegeln - IGEL OS Desktop über VNC beobachten (see page 481).

Beenden: Die UMS Konsole schließen.

Bearbeiten

In diesem Menü finden Sie Optionen zur Bearbeitung von markierten Objekten:



Beschreibungsdaten speichern: Speichern geänderter Daten des Inhaltsbereichs.

Konfiguration bearbeiten: Konfigurationsparameter des ausgewählten Geräts oder Profils bearbeiten.

Umbenennen: Objekt im Strukturbaum umbenennen.

Löschen: Objekt im Strukturbaum löschen.

Berechtigungen: Verwalten der Rechte am ausgewählten Objekt für Benutzer und Gruppen

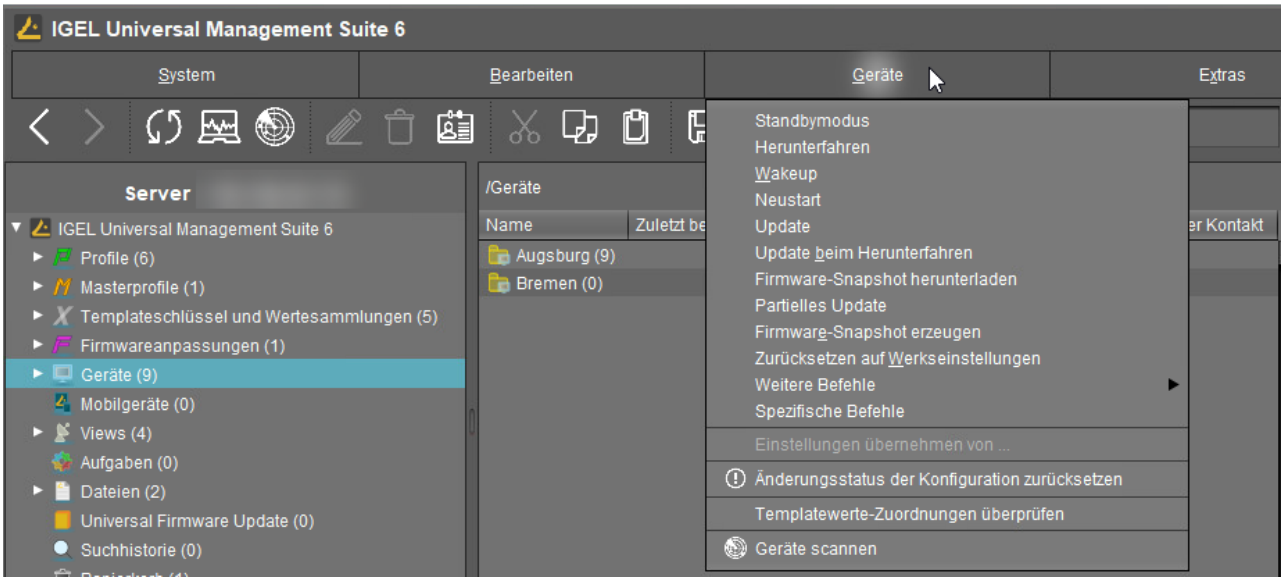
Ausschneiden: Datenobjekt ausschneiden und in die Zwischenablage kopieren.

Kopieren: Datenobjekte in die Zwischenablage kopieren.

Einfügen: Datenobjekte aus Zwischenablage einfügen.

Geräte

In diesem Menü finden Sie sämtliche Befehle, die an die ausgewählten Geräte gesendet werden können:



Die meisten dieser Befehle können auch über das Kontextmenü aufgerufen werden, d.h. über einen Rechtsklick auf ein einzelnes Gerät oder ein Geräteverzeichnis.

Standbymodus: Setzt die markierten Geräte in den Standbymodus.

Herunterfahren: Fährt die markierten Geräte herunter.

Wakeup: Startet die markierten Geräte über das Netzwerk (Wake-on-LAN).

Neustart: Führt bei den markierten Geräten einen Neustart durch.

Update: Führt bei den markierten Geräten mit IGEL OS ein Firmwareupdate aus.

Update beim Herunterfahren: Führt das Firmwareupdate beim Herunterfahren der markierten Geräten mit IGEL OS aus.

Firmware-Snapshot herunterladen: Lädt den Snapshot der Firmware für die markierten Windows-Clients herunter.

Partielles Update: Führt ein partielles Update auf den markierten Windows-Clients aus.

Firmware-Snapshot erzeugen: Erzeugt einen Snapshot der Firmware auf den markierten Windows-Clients.

Zurücksetzen auf Werkseinstellungen: Setzt die markierten Geräte auf die Werkseinstellungen zurück.

Siehe auch Reset to Factory Defaults (IGEL OS) oder Reset to Factory Defaults (Windows).

Weitere Befehle:

- **Nachricht senden**: Sendet eine Nachricht an die markierten Geräte.
- **Zurücksetzen auf Werkseinstellungen**: Setzt die markierte Geräte auf die Werkseinstellungen zurück.
- **Einstellungen UMS->Gerät**: Sendet die Konfiguration der UMS an die markierten Geräte.
- **Einstellungen Gerät ->UMS**: Liest die lokale Konfiguration der markierten Geräte in die UMS.
- **Desktopanpassungen aktualisieren**: Aktualisiert den eingestellten Bildschirmhintergrund und das Bootlogo auf den markierten Geräten mit IGEL OS.
- **Datei UMS ->Gerät**: Definiert eine Datei, die an die markierten Geräte gesendet wird.
- **Gerätedatei ->UMS**: Definiert eine Datei, die von den markierten Geräten an die UMS gesendet wird.
- **Flash Player herunterladen**: Lädt das Flash-Player-Plugin für Firefox auf die markierten Geräte mit IGEL OS.
- **Flash Player entfernen**: Entfernt das Flash-Player-Plugin für Firefox von den markierten Geräte mit IGEL OS.
- **Zertifikat speichern**: Speichert das UMS Zertifikat auf markierte Geräte.
- **Zertifikat entfernen**: Entfernt das UMS Zertifikat von den markierten Geräten. Siehe auch UMS Zertifikat vom OS 11 Gerät entfernen (see page 220).
- **Lizenzinformationen aktualisieren**: Die Lizenzinformationen werden aktualisiert.
- **Systeminformation aktualisieren**: Die Systeminformationen werden aktualisiert.
- **Asset Inventory Daten aktualisieren**: Asset Inventory Daten werden aktualisiert.

Spezifische Befehle: Führt die folgenden Befehle durch:

- **Installiere Jabra Xpress Paket**: Installiert ein Jabra Xpress Paket (IGEL OS).
- **Start Login Enterprise Launcher**: Startet den bereits konfigurierten Login PI Launcher, siehe Login Enterprise Launcher in IGEL OS.

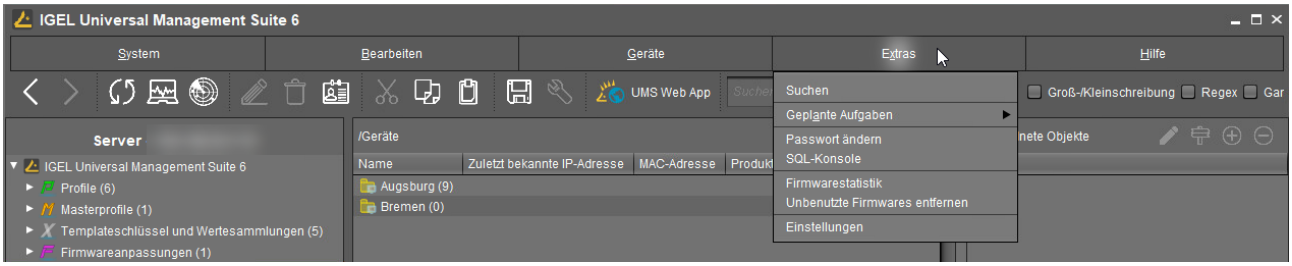
Einstellungen übernehmen von...: Sendet Profileinstellungen einmalig an das Gerät.

Änderungsstatus der Konfiguration zurücksetzen: Setzt die Änderungsmarkierungen (blauer Punkt an den Symbolen der Geräte) zurück.

Templatewerte-Zuordnungen überprüfen: Überprüft die Zuordnung von Templatewerten. Siehe Templateprofile und Werte den Geräten zuordnen (see page 429). Allgemeine Informationen zu Templateprofilen finden Sie unter Templateprofile in der IGEL UMS (see page 416).

Geräte scannen: Sucht nach Geräten im Netzwerk des UMS Servers.

Extras



Suchen: Suche nach Objekten - die Suche wird im Strukturbaum unter Suchhistorie (see page 543) aufgelistet und kann dort wieder verändert werden.

Geplante Aufgaben: Verwaltung von Feiertagslisten und Zuweisung von Aufgaben an Hosts

- **Hostzuweisung**: Virtuelle Hosts ausgewählten Geräten zuweisen.
  - **Universal Management Suite Host**: Hostname der UMS
  - **Letzter Scheduler-Lauf**: Datum und Uhrzeit vom letzten Lauf des Schedulers
  - **Verfügbare Geräte**: Eingrenzung der Anzeige von verfügbaren Geräten
  - **Zugewiesene Geräte**: Baum- oder Listenansicht der verfügbaren Geräte im ausgewählten Host

- **Feiertagslisten verwalten**: Festlegen von Feiertagslisten, die Sie beim Erstellen neuer Aufgaben verwenden können
  - **Datumslisten**: Anlagen von Listen für Feiertage
  - **Tage**: Festlegen des Datums der Feiertage in einer Feiertagsliste

Passwort ändern: Änderung des Passworts des angemeldeten Benutzers

SQL-Konsole: Direkter Zugriff auf die Datenbank mit SQL-Befehlen

> Die SQL-Konsole ist ausschließlich für administrative Zwecke vorgesehen. Sie können mit Operationen auf der SQL-Konsole die Datenbank zerstören.

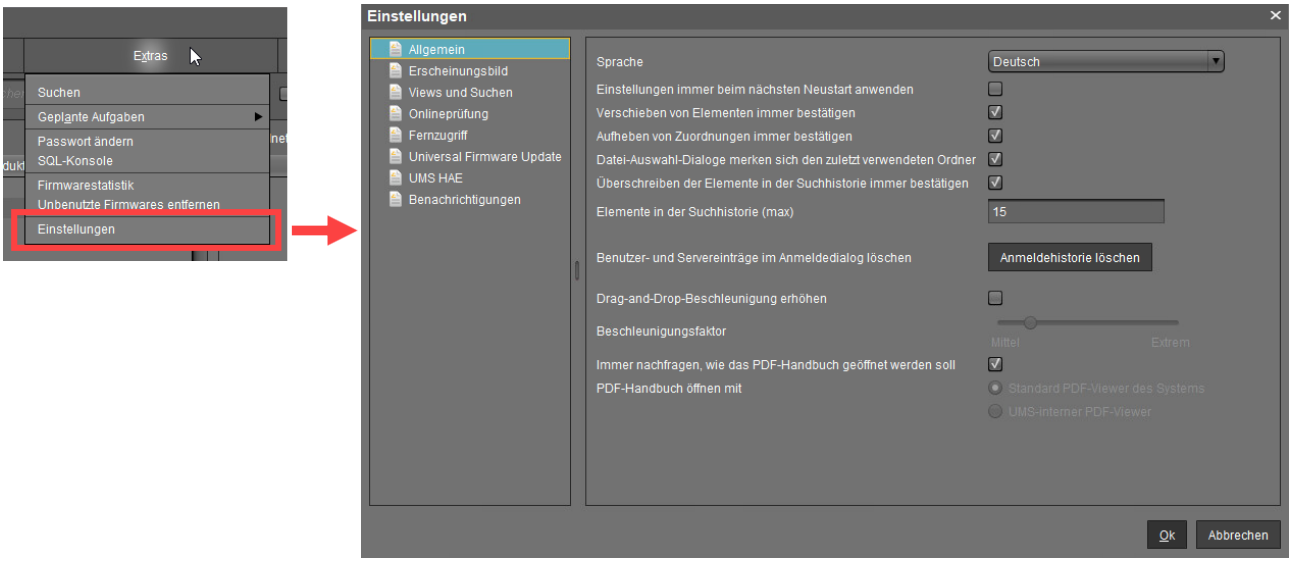
Firmwarestatistik: Auflistung der in der Datenbank registrierten Firmwareversionen mit Filterfunktion

Unbenutzte Firmwares entfernen: Öffnet einen Dialog, der unbenutzte Firmwares auflistet und einzeln sowie zusammen zum Löschen aus der Datenbank anbietet.

> Die Funktion **Unbenutzte Firmwares entfernen** entfernt NICHT die heruntergeladene Firmware von der **UMS Konsole >** Universal Firmware Update (see page 539).

Einstellungen: Konfigurationsparameter wie Sprache und Erscheinungsbild der UMS Konsole, Typen von Benachrichtigungen usw. Weitere Details finden Sie unten unter "Einstellungen".

Einstellungen



Hier können Sie folgende Parameter ändern:

Allgemein

Sprache: Sprachauswahl für die grafische Benutzeroberfläche. Damit die Änderungen übernommen werden können, müssen Sie die UMS Konsole schließen und erneut starten.

☐ **Einstellungen immer beim nächsten Neustart anwenden** (Standard)

☑ **Verschieben von Elementen immer bestätigen** (Standard)

☑ **Aufheben von Zuordnungen immer bestätigen** (Standard)

☑ **Datei-Auswahl-Dialoge merken sich den zuletzt verwendeten Ordner** (Standard)

☑ **Überschreiben der Elemente in der Suchhistorie immer bestätigen** (Standard)

Elemente in der Suchhistorie (max): Maximale Anzahl der Elemente, die die Suchhistorie anzeigen soll. (Standard: 15)

Benutzer- und Servereinträge im Anmeldedialog löschen: Anmeldehistorie löschen.

☐ **Drag-and-Drop-Beschleunigung erhöhen** (Standard)

Beschleunigungsfaktor: Ist nur einstellbar, wenn das obige Kontrollkästchen aktiviert wurde.

☑ **Immer nachfragen, wie das PDF-Handbuch geöffnet werden soll** (Standard)

PDF-Handbuch öffnen mit: Wenn das obige Kontrollkästchen deaktiviert ist, können Sie auswählen, wie das PDF-Handbuch geöffnet werden soll:

- **Standard PDF-Viewer des Systems**
- **UMS-interner PDF-Viewer**

Erscheinungsbild

Skin (Erscheinungsbild): Auswahl an möglichen Themen/Farbkombinationen, in denen die GUI dargestellt wird.

Mögliche Optionen:

- **Workspace** (Standard)
- **Smart Contrast**
- **Zinn**
- **Aschgrau**
- **Ozean**

Gerätebefehle immer im Hintergrund

☑ im Hintergrund. (Standard)

Nachrichtenfenster bei neuen Nachrichten automatisch öffnen

☑ Der Nachrichtenbereich im unteren Teil des UMS Konsolenfensters wird bei eingehenden Nachrichten automatisch geöffnet. (Standard)

Anzahl der Verzeichnisinhalte anzeigen

☑ wird angezeigt. (Standard)

Zustand des Baumes beim Einloggen wiederherstellen

☑ Der Strukturbaum wird wieder auf den Zustand, wie er bei der letzten Anmeldung war, zurückgesetzt. (Standard)

Für Kategoriewurzelknoten das Objekt-Icon verwenden

☑ Icons als Symbole für die Hauptkategorien im Strukturbaum anzeigen. (Standard)

☐ Ordnersymbole für die Hauptkategorien im Strukturbaum anzeigen.

Erweiterten Gerätezustand als Icon anzeigen

☑ In der UMS Konsole werden Symbole für den Gerätestatus angezeigt; siehe Geräte (see page 447). (Standard)

☐ Symbole für den Gerätestatus werden nicht angezeigt.

Der Verzeichnis-Tooltip zeigt den Verzeichnispfad

☑ wird angezeigt. (Standard)

Der Verzeichnis-Tooltip zeigt die Anzahl der Verzeichnisinhalte

☑ Im Tooltip wird die Anzahl der Verzeichnisse und der Objekte des Verzeichnisses angezeigt. (Standard)

Views und Suchen

Sie können die Anzeige der Ergebnisse von Views und die Anzeige von Suchergebnissen konfigurieren.

Aufbewahrungszeit für Views: Legt fest, wie lange die Ergebnisse von Views im Cache zwischengespeichert werden.

Mögliche Optionen:

- **Details werden niemals gespeichert**: Die Ergebnisse von Views werden nicht zwischengespeichert. Daher müssen sie jedes Mal erneut geladen werden, wenn die View im Strukturbaum unter **Views** ausgewählt wird. (Standard)
- **Details werden für [Zeitspanne] aufbewahrt**: Die Ergebnisse von Views werden für die angegebene Zeitspanne zwischengespeichert. Wenn die Zeitspanne abgelaufen ist, müssen die Ergebnisse der Views erneut geladen werden, sobald die View im Strukturbaum unter **Views** ausgewählt wird. Für die meisten Fälle wird die Option "Details werden für 30 Minuten aufbewahrt" empfohlen.

Aufbewahrungszeit für Suchen: Legt fest, wie lange die Ergebnisse von Suchen im Cache zwischengespeichert werden.

- **Details werden niemals gespeichert**: Die Suchergebnisse werden nicht zwischengespeichert. Daher müssen sie jedes Mal erneut geladen werden, wenn die Suche im Strukturbaum unter **Suchhistorie** ausgewählt wird. (Standard)
- **Details werden für [Zeitspanne] aufbewahrt**: Die Suchergebnisse werden für die angegebene Zeitspanne zwischengespeichert. Wenn die Zeitspanne abgelaufen ist, müssen die Suchergebnisse erneut geladen werden, sobald die Suche im Strukturbaum unter **Suchhistorie** ausgewählt wird. Für die meisten Fälle wird die Option "Details werden für 30 Minuten aufbewahrt" empfohlen.

Wenn eine View geladen wird...

Mögliche Optionen:

- **Automatisch Anzahl und Objekte laden**: Die Geräte werden sofort geladen, wenn eine View im Strukturbaum unter **Views** ausgewählt wird. Bei einer großen Anzahl von Geräten kann das hohe Ladezeiten nach sich ziehen. Sie können die Anzeige durch Klicken auf **Aktualisieren** auffrischen. (Standard)
- **Automatisch Anzahl laden**: Die Anzahl der Geräte wird sofort geladen, wenn eine View im Strukturbaum unter **Views** ausgewählt wird. Damit die Geräte angezeigt werden, klicken Sie auf **Geräte laden**.
- **Nur die Parameter anzeigen**: Nichts wird sofort geladen, wenn eine View im Strukturbaum unter **Views** ausgewählt wird. Damit die Geräte angezeigt werden, klicken Sie auf **Nach Treffern suchen** > **Geräte laden**.

Wenn ein Suchergebnis geladen wird...

Mögliche Optionen:

- **Automatisch Anzahl und Objekte laden**: Die Geräte / Profile / Views werden sofort geladen, wenn eine Suche im Strukturbaum unter **Suchhistorie** ausgewählt wird. Bei einer großen Anzahl von Geräten / Profilen / Views kann das hohe Ladezeiten nach sich ziehen. Sie können die Anzeige durch Klicken auf **Aktualisieren** auffrischen. (Standard)
- **Automatisch Anzahl laden**: Die Anzahl der Geräte / Profile / Views wird sofort geladen, wenn eine Suche im Strukturbaum unter **Suchhistorie** ausgewählt wird. Damit die Geräte / Profile / Views angezeigt werden, klicken Sie auf **Gerät laden** / **Profil laden** / **View laden**.
- **Nur die Parameter anzeigen**: Nichts wird sofort geladen, wenn eine Suche im Strukturbaum unter **Suchhistorie** ausgewählt wird. Damit die Geräte / Profile / Views angezeigt werden, klicken Sie auf **Nach Treffern suchen > Gerät laden** / **Profil laden** / **View laden**.

Treffermenge einer View im Baum anzeigen

☑ Die Anzahl der Geräte wird im Strukturbaum angezeigt, vorausgesetzt, die Anzahl wurde mindestens einmal geladen. (Standard)

☐ Die Anzahl der Geräte wird nicht angezeigt.

In Views zusätzlich Anzahl versteckter Geräte anzeigen

☑ Die Anzahl der versteckten Geräte wird im Strukturbaum angezeigt.

☐ Die Anzahl der versteckten Geräte wird nicht angezeigt. (Standard)

Onlineprüfung

Hier können Sie festlegen, wie oft die UMS die Geräte abfragt, um zu überprüfen, ob sie online sind.

Alle: Die Onlineprüfung wird im angegebenen Intervall in Millisekunden durchgeführt. (Standard: 3000)
Symbole, die den Online-Status anzeigen, finden Sie unter Geräte (see page 447).

Nie: Es wird keine Onlineprüfung durchgeführt.

Jetzt prüfen: Die Onlineprüfung wird ausgeführt, wenn diese Schaltfläche angeklickt wird.

Fernzugriff

Externer VNC-Viewer: Ermöglicht die Konfiguration eines externen VNC-Viewers mittels Eingabe oder Auswahl des Pfades zur ausführbaren Datei. Dies gilt nur für die UMS Konsole, nicht für die IGEL UMS Web App (see page 783).

Externer Terminal-Client: Ermöglicht den Auswahl eines externen Terminal-Clients mittels Eingabe oder Auswahl des Pfades zur ausführbaren Datei. (Derzeit unterstützt: Putty)

Beendedialog anzeigen, falls zwei oder mehr Sitzungen offen sind

☑ Dialog zum Beenden wird angezeigt. (Standard)

Warndialog für unerwartet beendete Sitzungen anzeigen

☑ Warndialog wird angezeigt. (Standard)

Universal Firmware Update

Automatische Aktualisierung des Status

☑ Der Status der Registrierung des Firmwareupdates wird automatisch aktualisiert. (Standard)

Intervall der Aktualisierung: Intervall in Sekunden. (Standard: 3)

UMS HAE

Hier können Sie die Statusaktualisierung der High-Availability-Erweiterung (see page 909) konfigurieren.

Die automatische Statusaktualisierung aktivieren

☑ Der Prozessstatus wird automatisch aktualisiert. (Standard)

Intervall der Statusaktualisierung: Intervall in Sekunden. (Standard: 30)

Die Statusanzeige sehen Sie im Inhaltsbereich, wenn Sie unter **UMS Administrator > Server** auf einen Server oder Load Balancer klicken.

Benachrichtigungen

Benachrichtigungen beim Start anzeigen

☑ Die Benachrichtigung wird automatisch bei jeder Konsolenverbindung angezeigt. (Standard)

☐ Die Benachrichtigung wird nicht automatisch angezeigt. Um die Benachrichtigung zu sehen, gehen Sie zu **Hilfe > Benachrichtigungen**.

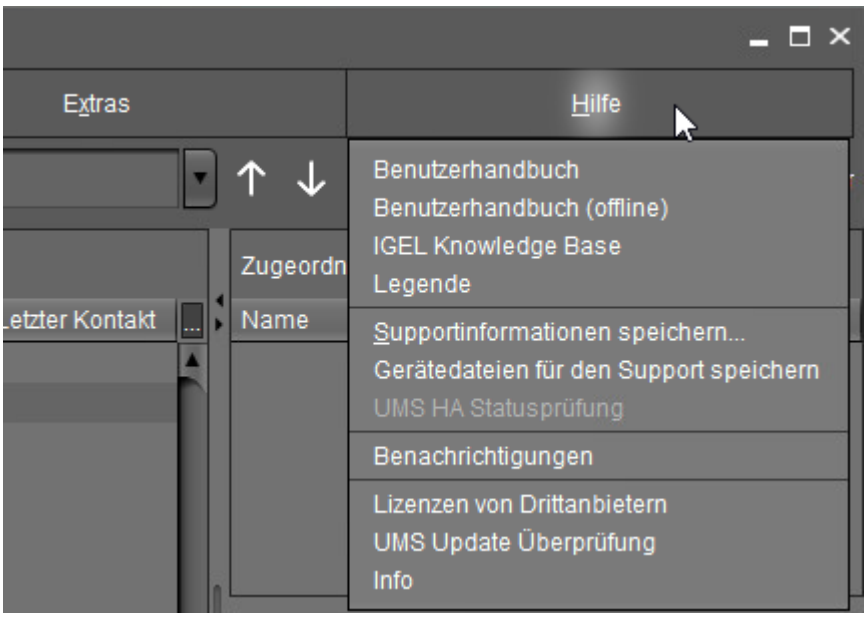
Zeige folgende Benachrichtigungen für den aktuellen Benutzer bzw. für die aktuelle Gruppe
Mögliche Werte:

- **Alle anzeigen**: Alle Benachrichtigungstypen werden angezeigt.
- **Nichts anzeigen**: Keine Benachrichtigungen werden angezeigt.
- **Benutzerdefiniert**: Sie können auswählen, welche Benachrichtigungstypen angezeigt werden sollen.

Einzelheiten zu den verschiedenen Benachrichtigungstypen finden Sie unter Benachrichtigungen in der IGEL UMS konfigurieren (see page 221).

Hilfe

In diesem Bereich erhalten Sie verschiedene Informationen, die Ihnen im Umgang mit der UMS helfen können.



Benutzerhandbuch: Link zum Handbuch auf kb.igel.com[27]

Benutzerhandbuch (offline): Öffnet das Benutzerhandbuch im PDF-Format.

27 http://kb.igel.com

IGEL Knowledge Base: Link zu weiterer Online-Dokumentation auf kb.igel.com[28]

Legende: Symbole, die in der UMS verwendet werden und ihre Bedeutung.

Supportinformation speichern...: Speichert Logdateien von UMS Server und UMS Konsole sowie Profile und zugehörige Firmware-Informationen der ausgewählten Geräte in einer ZIP-Datei und speichert ebenfalls alle Logdateien der verbunden ICGs. Ist die Erweiterung IGEL Management Interface (IMI) im Einsatz, wird auch deren API-Logdatei mit gespeichert. Weitere Informationen finden Sie unter Support-Assistent in der IGEL UMS (see page 702).

Gerätedateien für den Support speichern: Speichert Log- und Konfigurationsdateien eines Geräts, beispielsweise `setup.ini` und `group.ini` in einer ZIP-Datei.

UMS HA Statusprüfung: Prüft, ob die Interaktion zwischen den Komponenten des High-Availability-Systems funktioniert, insbesondere, ob die Komponenten Nachrichten und Daten austauschen können. Weitere Informationen finden Sie unter UMS HA Statusprüfung - Ihre High Availability- und Distributed UMS-Systeme analysieren (see page 944).

Benachrichtigungen: Liste aller bisher gesendeten Benachrichtigungen.

Lizenzen von Drittanbietern: Auflistung der Lizenzen von in der UMS verwendeter Fremdsoftware und Bibliotheken

UMS Update Überprüfung: Prüft, ob eine neuere Version von UMS zum Download bereitsteht.

Info: Anzeigen der aktuellen Version von UMS Konsole und Java-Umgebung sowie des angemeldeten Benutzers

28 http://kb.igel.com

Strukturbaum der IGEL UMS Konsole

Sie können Objekte im Strukturbaum der IGEL Universal Management Suite (UMS) Konsole durch Anklicken markieren bzw. auswählen. Eine Mehrfachauswahl ist mit [Umschalttaste] bzw. [Strg] möglich.

Sie können festlegen, ob sich die UMS Konsole die ausgeklappten Bereiche im Strukturbaum merken und beim nächsten Start bereits ausgeklappt anzeigen soll. Bei umfangreichen Strukturen kann das allerdings zu längeren Startzeiten führen. Die Einstellung **Zustand des Baumes beim Einloggen wiederherstellen** finden Sie unter **Extras** > **Einstellungen** > **Erscheinungsbild**.

Sie können auch die Beschleunigung beim Scrollen für Drag & Drop-Aktionen erhöhen. Die Beschleunigung startet, sobald das bewegte Objekt den unteren Rand des Fensters des Strukturbaums berührt. Eine höhere Beschleunigung ist sinnvoll, wenn der Strukturbaum sehr viele Objekte enthält. Um die Scrollgeschwindigkeit zu ändern, aktivieren Sie **Extras > Einstellungen > Allgemein > Drag-and-Drop-Beschleunigung erhöhen** und stellen Sie den **Beschleunigungsfaktor** auf einen geeigneten Wert ein.

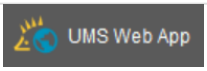
Hinter jedem Ordner ist die Anzahl der enthaltenen Elemente angegeben, einschließlich der Elemente in Unterordnern. Sie können diese Einstellung ändern unter **Extras** > **Einstellungen** > **Erscheinungsbild** > **Anzahl der Verzeichnisinhalte anzeigen**.

Der Strukturbaum gliedert sich in die folgenden Unterbereiche:

- Profile (see page 365): Erstellen und Organisieren der Standardprofile.
- Priority Profile (see page 413): Erstellen und Organisieren der Priority Profile.
- Templateschlüssel und Wertesammlungen (see page 416): Schlüssel und Werte zur Verwendung in Templateprofilen.
- Firmwareanpassungen (see page 435): Die Benutzeroberfläche an Ihr Corporate Design anpassen.
- Geräte (see page 447): Verwalteten Geräte organisieren.
- **Shared Workplace-Benutzer** (see page 488): Spezifische Profile an AD-Benutzern zuweisen.
- Views (see page 489): Konfigurierbaren Listenansichten von Geräten erstellen.
- Aufgaben - Senden von automatisierten Befehlen an Geräte in der IGEL UMS (see page 518): Zeitgesteuerte Aufgaben, wie z. B. Firmware-Updates, definieren.
- Dateien (see page 529): Dateien für die Übertragung an Thin Clients registrieren.
- Universal Firmware Update (see page 539): Aktuelle Firmwareversionen zur Verteilung an Geräte herunterladen.
- Suchhistorie (see page 543): Gespeicherte Suchanfragen.
- Papierkorb (see page 545): Gelöschte und wiederherstellbare Objekte.

Symbolleiste

In der **Symbolleiste** finden Sie Schaltflächen für häufig verwendete Befehle:

	In der Konsolenhistorie um einen Schritt vor oder zurück navigieren. Dies betrifft nur die Ansicht; Aktionen können nicht rückgängig gemacht werden.
	Ansicht und des Status der Geräte aktualisieren
	Onlineprüfung der Geräte
	Im Netzwerk nach Geräten suchen
	Objektnamen im Strukturbaum ändern
	Objekte im Strukturbaum löschen
	Zugriffsrechte für ausgewählte Objekte festlegen
	Ein Baumelement ausschneiden und in die Zwischenablage verschieben
	Ein Baumelement in die Zwischenablage kopieren
	Ein Baumelement aus der Zwischenablage einfügen
	Bearbeitete Beschreibungsdaten von Geräten oder Profilen speichern
	Konfigurationsparameter von Geräten oder Profilen bearbeiten
	Die IGEL UMS Web App (see page 783) öffnen
	Objekte im Strukturbaum anhand von Namen, MAC, IP oder ID finden. Reguläre Ausdrücke (**Regex**) lassen sich verwenden; die letzten 20 Suchanfragen des Benutzers werden gespeichert.

	In den Suchergebnissen um einen Schritt vor oder zurück navigieren
Groß-/Kleinschreibung	Festlegen, ob bei der Suche die Groß- und Kleinschreibung berücksichtigt wird
Regex	Festlegen, ob bei der Suche reguläre Ausdrücke verwendet werden
Ganzer Text	Festlegen, ob der Suchausdruck mit dem gesamten Text übereinstimmen muss oder nur mit einem Teil davon

Inhaltsbereich der IGEL UMS Konsole

Der Inhaltsbereich, oder Content Panel der IGEL Universal Management Suite (UMS) Konsole, zeigt die Eigenschaften des jeweils im Strukturbaum markierten Objekts an. Dies kann der Inhalt eines Verzeichnisses sein, also z. B. die dort abgelegten Profile, Geräte, Unterordner, Aufgaben usw., oder Detailinformationen eines Objekts, wie Systeminformationen des Geräts, Basisdaten eines Profils, Trefferliste einer View usw.

Beispielliste von Details, die im Inhaltsbereich für einige Objekte des UMS Strukturbaums angezeigt werden

Server - [IP-Adresse]

- **Profile**: Name, Beschreibung, Profil ID usw. Siehe Profile in der IGEL UMS (see page 365).
- **Priority Profile**: Name, Beschreibung, Profil ID usw. Siehe Priority Profile in der IGEL UMS (see page 413).
- **Templateprofile**: Name und Beschreibung der Templateschlüssel und Wertesammlungen. Siehe Templateprofile in der IGEL UMS (see page 416).
- **Firmwareanpassungen**: Name, Anwendungsfall und Konfigurationsparameter einer Firmwareanpassung. Siehe Firmwareanpassungen in der IGEL UMS (see page 435).
- **Geräte**: Systeminformationen, Lizenz- und Monitorinformationen, Features usw. Siehe Geräte (see page 447) und Geräteinformationen in der IGEL UMS einsehen (see page 449).

  > Mit der Schaltfläche **Daten in Zwischenablage kopieren (ASCII)**, die sich unten im Inhaltsbereich befindet, können Sie die Geräteinformationen im ASCII-Format kopieren.

- **Shared Workplace-Benutzer**: Name, E-Mail-Adresse der Benutzer aus Active Directory usw. Siehe Shared Workplace-Benutzer (see page 488).
- **Views**: Name, Regel, gefundene Geräte usw. Siehe Views (see page 489).
- **Aufgaben**: Aufgaben-Info, Zeitplan, Ergebnisse usw. Siehe Aufgaben - Senden von automatisierten Befehlen an Geräte in der IGEL UMS (see page 518).
- **Dateien**: Ursprungs-URL, Klassifizierung, Speicherpfad des Geräts, Zugriffsrechte usw. Siehe Dateien - Dateien am IGEL UMS Server registrieren und zu Geräten übertragen (see page 529).
- **Universal Firmware Update**: Einstellungen der Firmwareupdates, Downloadstatus usw. Siehe Universal Firmware Update (see page 539).
- **Suchhistorie**: Name, Regel, gefundene Objekte usw. Siehe Suchhistorie (see page 543).
- **Papierkorb**: Name und Typ des gelöschten Objekts, sein Löschdatum usw. Siehe Papierkorb - Löschen von Objekten in der IGEL UMS (see page 545).

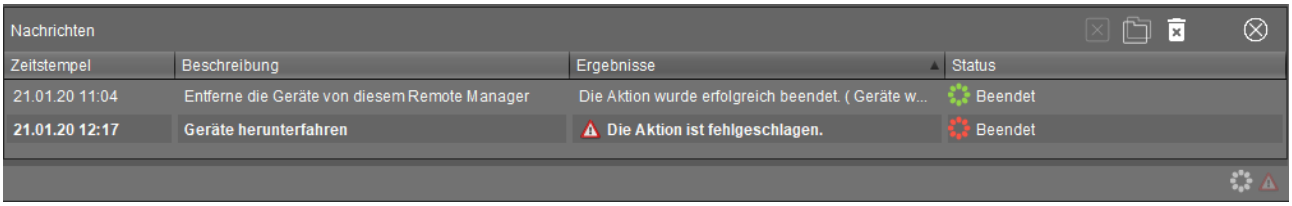
UMS Administration

- **Server**: Informationen zum ausgeführten Dienst, Anfragen, abgewiesene und wartende Anfragen. Siehe Server - Informationen zu Ihrem UMS Server anzeigen (see page 551).
- **Load Balancer**: Informationen zum ausgeführten Dienst, Anfragen, abgewiesene und wartende Anfragen. Siehe Load Balancer - Informationen zu Ihrem IGEL UMS Load Balancer anzeigen (see page 554).
- **Lizenzen**: Lizenzüberblick, registrierte Lizenzen. Siehe Lizenzen (see page 560).

- **Zertifikatsverwaltung**: Signaturalgorithmus, Schlüssel, Zustand der Zertifikate usw. Siehe Zertifikatsverwaltung (see page 572).
- **Geräteattribute**: Attributname, -typ usw. Siehe Geräteattribute für IGEL OS Geräte verwalten (see page 593).
- **Administrative Aufgaben**: Liste mit Aufgaben, Ausführungsprotokoll. Siehe Administrative Aufgaben - Zeitlich geplante Aktionen für die IGEL UMS konfigurieren (see page 597).
- **Proxyserver**: Name, Rechnername, Port usw. Siehe Proxyserver (see page 641).
- **Universal Firmware Update**: Einstellungen des Universal Firmware Updates, Einstellungen des FTP-Servers, auf den die Dateien kopiert werden (optional). Siehe Universal Firmware Update (1) (see page 357).
- **Wake-on-LAN**: Wake-on-LAN-Konfigurationsparameter. Siehe Wake-on-LAN (see page 654).
- **Active Directory / LDAP**: Active Directory / LDAP-Domänen. Siehe Active Directory / LDAP (see page 657).
- **Fernzugriff**: Sichere VNC-Verbindung, grafische Einstellungen usw. Siehe Fernzugriff (see page 659).
- **Logging**: Nachrichten-Log-Einstellungen, Ereigniseinstellungen aufzeichnen. Siehe Logging (see page 661).
- **E-Mail-Einstellungen**: E-Mail-Einstellungen, Empfänger für die Ergebnis-E-Mails der administrativen Aufgaben und Service E-Mails. Siehe E-Mail-Einstellungen (see page 664).
- **UMS Features**: Papierkorb, Templateprofile, Priority Profile, usw. aktivieren. Siehe UMS Features (see page 669).

Nachrichten

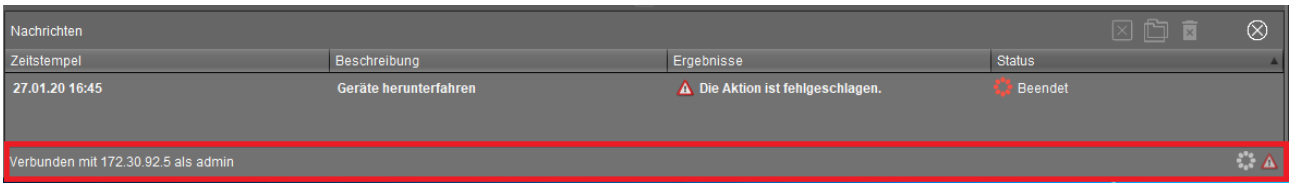
Der Fensterbereich **Nachrichten** enthält Informationen über die erfolgreiche oder fehlerhafte Ausführung von Befehlen. Wenn ein Kommando nicht erfolgreich ausgeführt werden konnte, wird dies in der **Nachrichten**-Liste durch ein Warnzeichen und ein rotes **Status**-Symbol markiert. Außerdem blinkt ein Warnzeichen in der Statuszeile der UMS Konsole, bis der Benutzer die Nachricht auswählt.



- Klicken Sie oder doppelklicken Sie die Nachricht, um Details zur Nachricht anzusehen.
- Klicken Sie , um gelesene Nachrichten zu löschen, oder warten Sie, bis das Nachrichtenfenster beim Beenden der UMS Konsole automatisch zurückgesetzt wird.
- Ändern Sie die Größe des Nachrichtenfensters über den mittleren Slider oder blenden Sie es durch einen Klick auf ganz aus. Um den Fensterbereich **Nachrichten** wieder zu öffnen, klicken Sie in der Statuszeile der UMS Konsole (oder , falls Nachrichten über die fehlgeschlagene Befehlsausführung noch nicht ausgewählt wurden).

Statuszeile

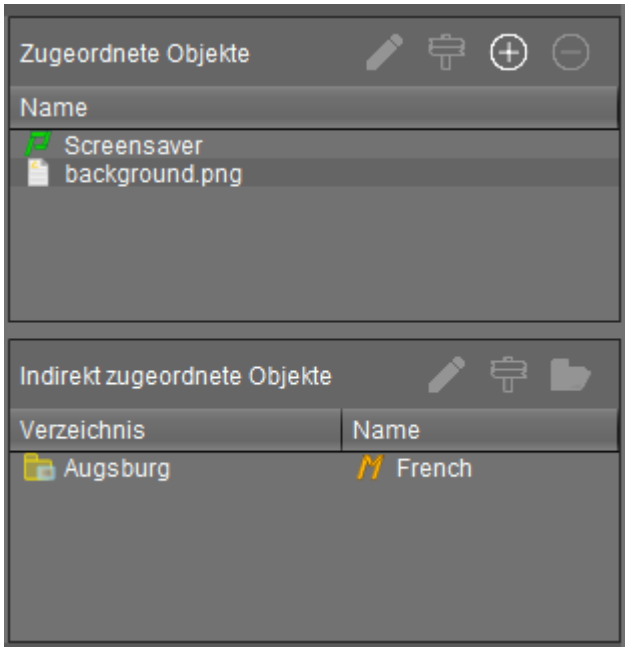
Die **Statuszeile** zeigt den Namen des aktuell verbundenen UMS Servers und des an der UMS Konsole angemeldeten Benutzers an. Das Symbol unten rechts signalisiert den Status des Nachrichtenfensters. Zum Beispiel zeigt es an, wenn neue Warnmeldungen vorhanden sind. An dieser Stelle sind sie auch bei ausgeblendetem Nachrichtenbereich zu sehen.



Zugeordnete Objekte

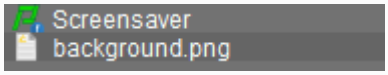
Der Bereich **Zugeordnete Objekte** gliedert sich in zwei Teile, um direkt von indirekt zugewiesenen Objekten schnell unterscheiden zu können:

- Direkt zugeordnete Objekte wurden einem einzelnen Gerät, Ordner oder Profil zugewiesen.
- Indirekte Objekte wurden über die Ordnerstruktur 'geerbt'.



▶ Doppelklicken Sie auf ein Objekt im Zuweisungsbereich, um es direkt editieren zu können.

Zugewiesene Objekte mit noch nicht an das Gerät übertragenen Konfigurationsänderungen werden mit einem Ausrufezeichen markiert:



Kontextmenü

Ein objektabhängiges **Kontextmenü** erhalten Sie durch Rechtsklick auf das entsprechende Objekt. Je nach Auswahl stehen Aktionen für Ordner, Geräte, Shared Workplace Benutzer usw. zur Verfügung. Das gewählte Kommando wird für alle zuvor im Baum markierten Objekte ausgeführt.

Manche Kommandos lassen sich nur für einzelne Objekte, nicht aber für Verzeichnisse mit Objekten ausführen. Diese Optionen sind im Menü dann deaktiviert. Beispiel: Das Kommando **Gerätedatei > UMS** kann nur für ein einzelnes Gerät ausgeführt werden, das Kommando **Datei UMS > Gerät** hingegen für alle Geräte in einem Verzeichnis.

Gerätebefehle

Sie können einen Befehl an ein Gerät nicht nur über das Kontextmenü, sondern auch über Menüleiste > **Geräte** (see page 343) senden.

Suche nach Objekten in der UMS

Objekte innerhalb des UMS Strukturbaums lassen sich über folgende Wege finden:

- **Quick Search**
- **Suchfunktion**
- **View**

Quick Search

Die **Quick Search**  in der Symbolleiste (see page 355) bietet den schnellsten Zugriff auf die Suchfunktion. Die Eingabemaske ist im Konsolenfenster immer sichtbar. Die Tastenkombination [Umschalt-Strg-F] setzt den Cursor direkt in das Eingabefeld. Die Suchanfragen der **Quick Search** sind begrenzt auf wenige Objekteigenschaften, z. B. Objektname, Objekt-ID, MAC- oder IP-Adresse. Diese Daten werden zum Start der UMS Konsole lokal gepuffert und sind somit ohne Datenbankzugriff sehr schnell durchsuchbar. Die letzten 20 Suchanfragen des Benutzers werden für den schnellen Zugriff gespeichert - allerdings nicht in der UMS Datenbank, sondern in den Systembenutzerdaten des Konsolenbenutzers (Windows Registry).

Suchfunktion

Die normale Suchfunktion der UMS (Menü **Extras > Suchen** oder Tastenkombination [Strg-F]) stellt umfangreiche Optionen zur Suche auf der UMS Datenbank bereit. Neben den Quick Search-Daten (s.o.) stehen hier auch alle anderen Daten von Geräten, Profilen oder Views zur Auswahl - z. B. die selbst vergebene Inventarnummer oder das Modell des angeschlossenen Monitors. Verschiedene Kriterien lassen sich logisch verknüpfen (UND / ODER). Die Suchanfragen des Benutzers werden im Strukturbaum unter **Suchhistorie** (see page 543)abgelegt und lassen sich so einfach bearbeiten und erneut verwenden.

Views

Sehr ähnlich wie Suchanfragen funktionieren Views (see page 489), auch hier lassen sich verschiedene Kriterien verknüpfen und die Anfrage speichern. Anders als Suchanfragen stehen Views jedoch allen UMS Administratoren - abhängig von ihren Berechtigungen - gemeinsam zur Verfügung. Außerdem lassen sich Views auch in die Definition geplanter Aufgaben (see page 518) einbinden.

Sowohl Suchergebnisse wie auch Views lassen sich ab UMS Version 5.02.100 mit Profilen belegen. Siehe dazu auch Einer View Objekte zuordnen (see page 517) und Objekte zu den Geräten von Views oder Geräte-Suchen zuordnen (see page 627).

Profile in der IGEL UMS

In der IGEL Universal Management Suite können Sie Profile erstellen und verwalten. **Profile** sind vordefinierte Konfigurationen, die Sie global über die UMS den verwalteten Geräten zuweisen können.

Menüpfad: **UMS Konsole > Profile**

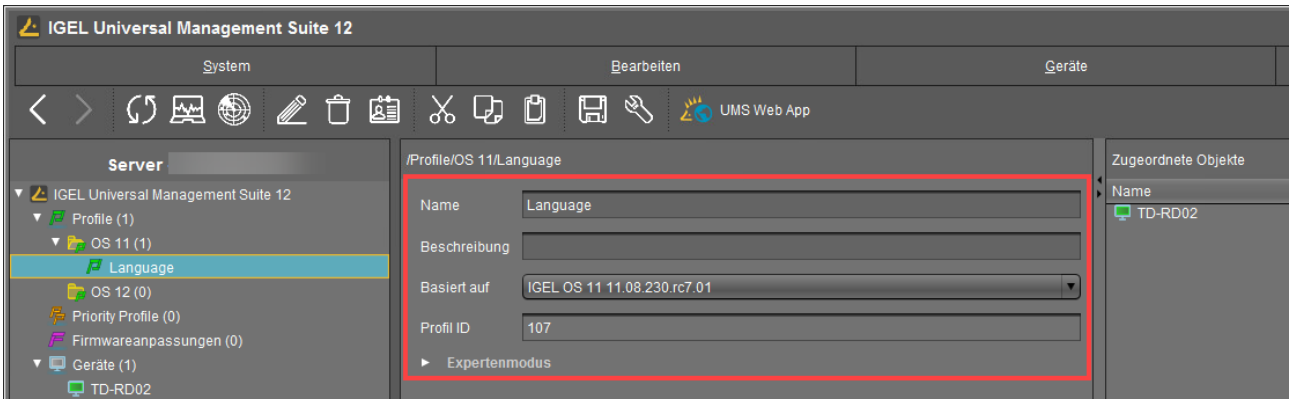
Wann ist es sinnvoll, Profile einzusetzen?

Folgendes können Sie durch den Einsatz von Profilen erreichen:

- Identische Konfigurationen für mehrere Geräte setzen
- Unterschiedliche Anwendungsszenarien von Geräten (oder Gruppen von Geräten) abstrakt abbilden
- Administrationsaufwand erheblich verringern
- Konfigurationsmöglichkeiten am Gerät reduzieren

Sie haben die Möglichkeit, Verzeichnisse zum Speichern von Profilen zu erstellen und können die Profile in diesem Teil der Struktur hinzufügen, löschen und ändern.

Die Informationen zu einem Profil werden im Inhaltsbereich angezeigt:



> Wer mit Active-Directory-Strukturen vertraut ist, kann ein Profil mit einer Richtlinie (Policy) vergleichen. Die Verzeichnisse, über die die Geräte gruppiert und verwaltet werden, entsprechen den Organisationseinheiten (Organisational Units) im AD.

Profiltypen

Es gibt folgende Profiltypen:

	**Standardprofile** können den Geräten **direkt** oder auch **indirekt** über Verzeichnisse zugewiesen werden. Ein Gerät kann seine Einstellungen von mehreren direkt oder indirekt zugewiesenen Profilen bekommen. Bei der Zuweisung überschreiben die Profileinstellungen die direkt am Gerät vorgenommenen Einstellungen. Siehe dazu Wirksamkeit der Einstellungen (see page 370). Wenn Sie Shared Workplace (see page 951) benutzen, haben Sie die Möglichkeit, Profile Benutzern zuzuordnen. Profile, die Benutzern zugewiesen sind haben höhere Priorität als Profile, die Geräte zugewiesen sind. Siehe dazu Wirkungsordnung der Profile in IGEL Shared Workplace (see page 402) und Wirkungsordnung der Profile (see page 398).
	**Templateprofile** sind Profile, bei denen eine oder mehrere Einstellungen über Variablen gesetzt werden. Diese Werte werden dynamisch ermittelt. Hierdurch lassen sich Standardprofile und Priority Profile noch flexibler einsetzen und kombinieren. Siehe dazu Kapitel Templateprofile in der IGEL UMS (see page 416). Wenn Sie Shared Workplace (see page 951) benutzen, beachten Sie, dass Templateprofile nicht verwendet werden können.
	**Priority Profile** können Einstellungen von Standardprofilen überschreiben und besitzen eigene Berechtigungen, siehe Priority Profile in der IGEL UMS (see page 413). Die Wirkungsordnung verläuft genau anders herum als bei den Standardprofilen. Siehe dazu Wirkungsordnung von Priority Profilen (see page 404).

Profile für IGEL OS 12 und IGEL OS 11 Geräte

- Das Verfahren zur Erstellung von Profilen für IGEL OS 12 Geräte und IGEL OS 11 Geräte ist unterschiedlich. Wenn Sie z. B. Chromium Browser-Einstellungen für Ihre IGEL OS 12 und IGEL OS 11 Geräte konfigurieren möchten, müssen Sie zwei Profile erstellen – ein Profil für OS 12 Geräte und ein anderes für OS 11 Geräte.
- Profile für IGEL OS 12 Geräte können nur in der UMS Web App erstellt und geändert werden. Es ist nicht möglich, sie in der UMS Konsole zu erstellen/bearbeiten.
- Profile für IGEL OS 11 Geräte können in der UMS Konsole und in der UMS Web App erstellt und bearbeitet werden.
- Direkte Zuweisung von OS 12-Profilen zu OS 11-Geräten ist nicht möglich, und umgekehrt. Wenn Sie ein OS 12-Profil einem OS 11-Gerät indirekt zuweisen, d.h. über eine Verzeichnisstruktur, werden die Einstellungen vom OS 12-Profil für das OS 11-Gerät NICHT berücksichtigt (und umgekehrt).

Dieses Kapitel erklärt, was Profile sind und wie sie funktionieren, und beschreibt, wie Profile in der UMS Konsole erstellt und verwaltet werden können. Details zu Profilen in der UMS Web App finden Sie unter Konfiguration - Zentralisierte Verwaltung von Geräteeinstellungen in der IGEL UMS Web App (see page 828).

- Priorisierung von Profilen in der IGEL UMS (see page 398)

IGEL Tech Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=Sc38mRv5Z1s&t=2s

Wahl des richtigen Profils

Standardprofile

Standardprofile reichen in den allermeisten Fällen aus, um Konfigurationseinstellungen global zu definieren und über Profile auf Geräte zu übertragen. Sie können mehrere Profile gleichzeitig anwenden. Mit Hilfe der Prioritätenregelung lässt sich die Wirkungskraft der durch ein Profil vorgegebenen Parameterwerte steuern.

Im Kapitel Profile verwenden (see page 371) erfahren Sie, wie Sie Profile einrichten und zuweisen.

Im Kapitel Templateprofile in der IGEL UMS (see page 416) erfahren Sie außerdem, wie Sie Profile mit variablen Werten erstellen können.

Im Kapitel Priorisierung von Profilen in der IGEL UMS (see page 398) ist die Prioritätenregelung beschrieben.

Priority Profile

Bei einer hierarchischen Struktur mit verschiedenen Administratoren und komplexer Rechteverwaltung kann der Einsatz von einem oder zwei **Priority Profilen** hilfreich sein. Mit einem Priority Profil kann ein höherrangiger Administrator Profileinstellungen von anderen Administratoren beeinflussen, ohne diesen die Verwaltungsrechte zu entziehen.

Lesen Sie sich sehr genau das Kapitel Priority Profile in der IGEL UMS (see page 413) durch, bevor Sie diesen Profiltyp einsetzen.

> Setzen Sie **Priority Profile** ganz gezielt und sparsam ein. Bei falschem Gebrauch können Sie damit unbeabsichtigt alle anderen Profile außer Kraft setzen.

Benutzerspezifische Profile

Beim Einsatz von IGEL Shared Workplace (SWP) ist es sinnvoll, benutzerspezifische Konfiguration über Profile zu verwalten. Benutzerspezifische SWP-Profile unterscheiden sich in ihrer Wirkungsweise von Geräte-Profilen.

Lesen Sie dazu IGEL Shared Workplace - Benutzerprofil zuweisen (see page 955) und Im Benutzerprofil konfigurierbare Parameter (see page 959).

Konfigurationsebenen

Profile machen es möglich, Konfigurationsparameter an den IGEL OS Geräten global zu steuern.

Dafür ist wichtig zu verstehen, dass es Parameter für unterschiedliche Arten von Instanzen gibt, normale Parameter und Parameter für feste und freie Instanzen.

Normale Parameter und feste Instanzen

Als feste Instanzen bezeichnen wir Einstellungsmöglichkeiten, die fest im System integriert sind. Zu diesen festen Instanzen gehören z. B. Spracheinstellungen, Monitoreinstellungen, Einstellungen zum Firmwareupdate, zur Benutzeroberfläche etc. Diese Optionen können nicht hinzugefügt oder gelöscht, sondern nur verändert werden.

Parametereinstellungen von festen Instanzen, die direkt am Gerät vorgenommen wurden, können überschrieben werden, wenn in einem zugewiesenen Profil andere Werte vorgegeben werden. Werden feste Instanzen über verschiedene Profile gesteuert, gelten ganz bestimmte Priorisierungsregeln (see page 398).

Freie Instanzen

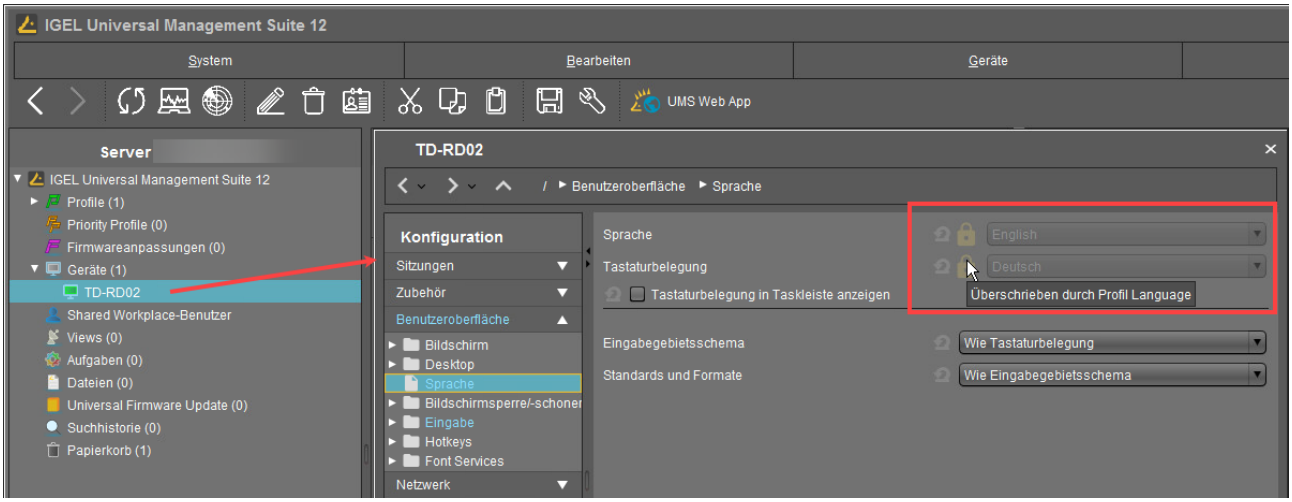
Hiermit sind die Instanzen gemeint, die der Benutzer über  hinzufügen oder löschen kann. Dazu gehören Sitzungen, USB-Geräte, Drucker, Zubehör, VPN-Verbindungen und alles, was in Gerätelisten auszuwählen ist.

Parameterwerte von freien Instanzen können nicht überschrieben werden. Werden einem Gerät mehrere freie Instanzen (z. B. Drucker) zugewiesen, addieren sie sich. Für die Parameterwerte der freien Instanzen gibt es daher keine Priorisierungen.

> Diese Regel können Sie brechen, wenn Sie bei der Einrichtung eines Profils **Sitzungen überschreiben** aktivieren, siehe Profile in der IGEL UMS erstellen (see page 372).

Wirksamkeit der Einstellungen

Parameterwerte, die durch ein Profil vorgegeben werden, sind im Konfigurationsdialog in der UMS sowie im IGEL Setup gesperrt und mit einem Schloss-Symbol gekennzeichnet.



Diese gesperrten Einstellungen können nur im Profil bearbeitet werden. Der Name des sperrenden Profils wird im Tooltip angezeigt.

Es gibt zwei Quellen, über die ein Parameterwert seine Einstellung erhält:

- über die Konfiguration direkt am Gerät und
- über die Vorgaben von Profilen

Die durch Profile bestimmten Werte haben Priorität.

> ⓘ Wenn Sie in einem Profil einen Wert für einen Parameter gesetzt haben und die Zuweisung zu einem Gerät aufheben, wird der Wert des Parameters in seinen vorherigen Wert geändert. Der Wert des Profils wird nicht in die Einstellungen des Geräts kopiert.

Profile verwenden

In diesem Kapitel erfahren Sie Folgendes:

Profile in der IGEL UMS erstellen

Im folgenden Artikel wird beschrieben, wie Sie Profile in der UMS Konsole erstellen können. Außerdem finden Sie hier Informationen über die Option **Sitzungen überschreiben** sowie über andere Expertenmodus-Einstellungen für Profile.

Wie Sie Profile in der UMS Web App erstellen können, erfahren Sie unter Profile in der IGEL UMS Web App erstellen und zuweisen (see page 838).

Menüpfad: **UMS Konsole > Profile**

Profile für IGEL OS 12 und IGEL OS 11 Geräte

- Das Verfahren zur Erstellung von Profilen für IGEL OS 12 Geräte und IGEL OS 11 Geräte ist unterschiedlich. Wenn Sie z. B. Chromium Browser-Einstellungen für Ihre IGEL OS 12 und IGEL OS 11 Geräte konfigurieren möchten, müssen Sie zwei Profile erstellen – ein Profil für OS 12 Geräte und ein anderes für OS 11 Geräte.
- Profile für IGEL OS 12 Geräte können nur in der UMS Web App erstellt und geändert werden. Es ist nicht möglich, sie in der UMS Konsole zu erstellen/bearbeiten.
- Profile für IGEL OS 11 Geräte können in der UMS Konsole und in der UMS Web App erstellt und bearbeitet werden.
- Direkte Zuweisung von OS 12-Profilen zu OS 11-Geräten ist nicht möglich, und umgekehrt. Wenn Sie ein OS 12-Profil einem OS 11-Gerät indirekt zuweisen, d.h. über eine Verzeichnisstruktur, werden die Einstellungen vom OS 12-Profil für das OS 11-Gerät NICHT berücksichtigt (und umgekehrt).

Um sicherzustellen, dass Sie alle neuen Features von IGEL OS nutzen können:

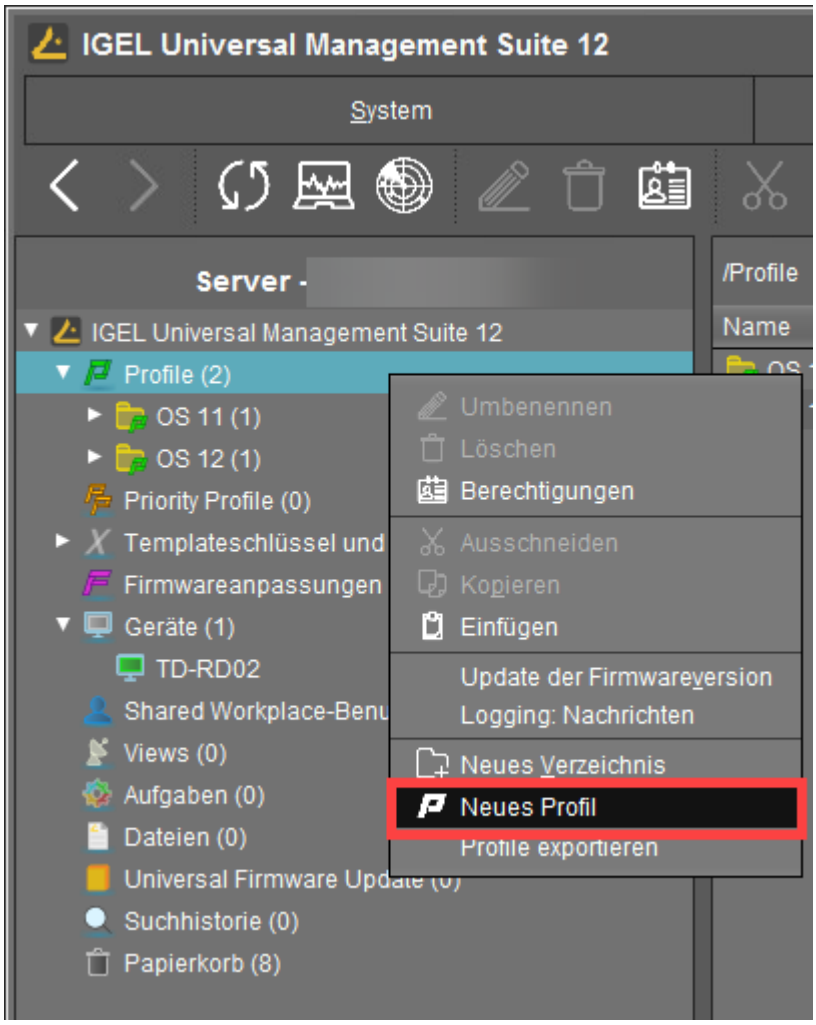
- Aktualisieren Sie Ihre UMS auf die neueste Version.
- Wählen Sie bei allen relevanten OS 11-Profilen (see page 372) für **Basiert auf** die passende Firmwareversion.
- Für OS 12-Profile (see page 838) ist Folgendes zu beachten: Ein OS 12-Profil konfiguriert ALLE Versionen einer App, solange nicht eine bestimmte Version unter **Versionen anzeigen** festgelegt ist.

Zur besseren Orientierung können Sie Unterverzeichnisse erstellen, um Ihre Profile anzuordnen.

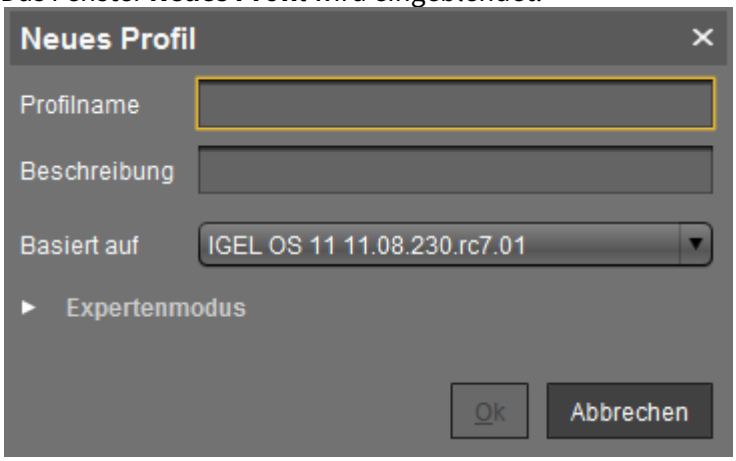
Ein Profil anlegen

So erstellen Sie ein neues Profil:

1. Klicken Sie in der UMS Konsole **Profile > [Kontextmenü] > Neues Profil** oder **System > Neu > Neues Profil**.
   Alternativ können Sie ein zuvor erstelltes Profil importieren. Siehe Profile exportieren und importieren (see page 390).



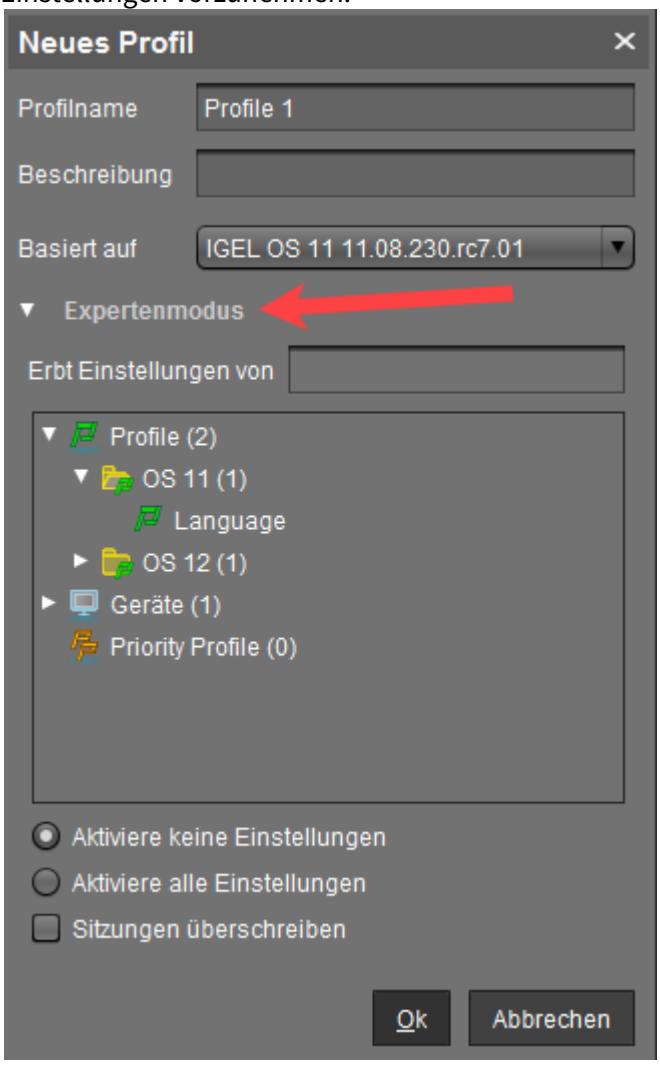
Das Fenster **Neues Profil** wird eingeblendet.



2. Geben Sie einen **Namen** und eine **Beschreibung** ein.

3. Wählen Sie unter **Basiert auf** eine Firmware-Version für das neue Profil aus.

4. Optional (normalerweise nicht erforderlich): Klicken Sie auf **Expertenmodus**, um die folgenden Einstellungen vorzunehmen:



- **Erbt Einstellungen von**: Hier können Sie festlegen, ob das neue Profil Einstellungen von einem bestehenden Profil oder Gerät übernehmen soll. Wenn ja, wählen Sie das erforderliche Profil / Gerät aus der Liste aus.

- **Aktiviere keine Einstellungen**: Es gibt zunächst keine aktiven Parameter. (Standard)
- **Aktiviere alle Einstellungen**: Alle verfügbaren Parameter des Profils sind aktiv.

- **Sitzungen überschreiben**: Alle freien Instanzen werden durch das Profil überschrieben.

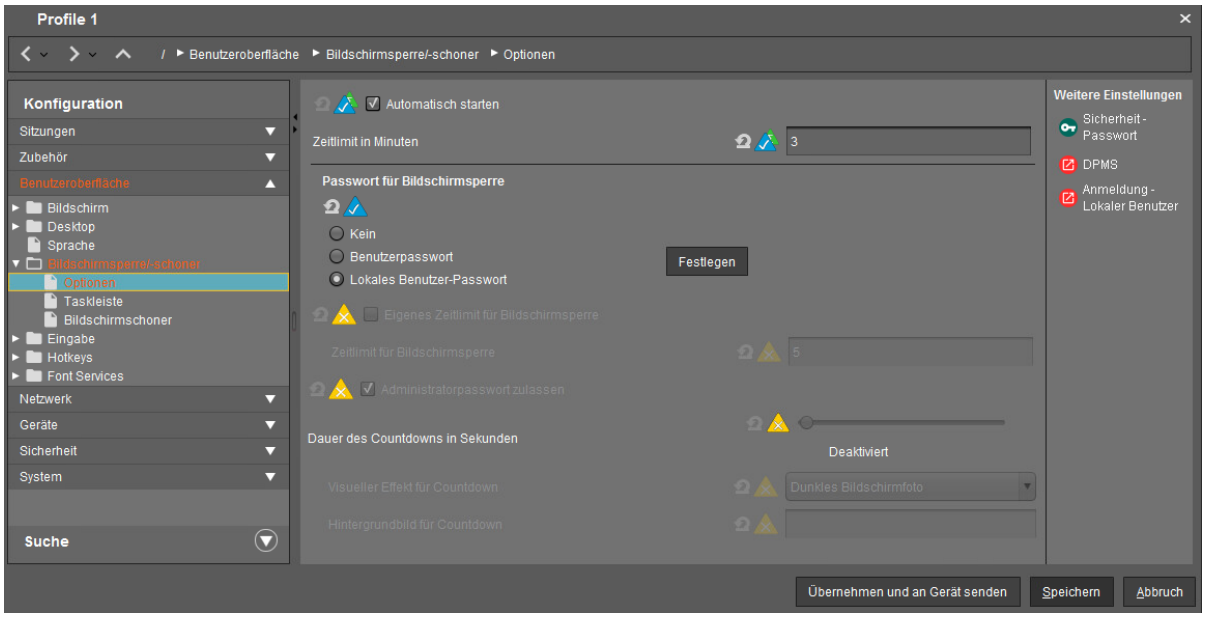
> **ACHTUNG!** Bevor Sie die Standardeinstellungen hier ändern, informieren Sie sich über die möglichen Auswirkungen unten unter "Neues Profil: Expertenmodus". **Aktiviere alle Einstellungen** wird alle Einstellungen im lokalen Setup blockieren! **Sitzungen überschreiben** sollte nur in Ausnahmefällen aktiviert werden! Mit dieser Option können Sie freie Instanzen aller anderen Profile überschreiben.

5. Klicken Sie **OK**, um das Profil einzurichten und zu speichern.

   > Das neue Profil wird im selektierten Profilverzeichnis hinterlegt. Wurde keins ausgewählt, wird es direkt im Verzeichnis **Profile** abgelegt.

6. Konfigurieren Sie die gewünschten Einstellungen.
   Um Einstellungen zu ändern, klicken Sie das Aktivierungssymbol vor dem Parameter, bis die gewünschte Funktion aktiv ist.

	Der Parameter ist inaktiv und wird nicht durch das Profil konfiguriert.
	Der Parameter ist aktiv und wird durch das Profil konfiguriert. Die Templateschlüssel sind inaktiv.
	Parameter auf Standardwert zurücksetzen.
Die folgenden Aktivierungssymbole werden nur angezeigt, wenn Templateprofile aktiviert sind (siehe Templateprofile in der IGEL UMS (see page 416)):	
	Der Parameter ist aktiv und wird durch das Profil konfiguriert. Die Templateschlüssel sind aktiv.
	Der Parameter ist aktiv und wird durch das Profil konfiguriert. Der Parameter wird aus einem Templateschlüssel bezogen.



7. Speichern Sie die Einstellungen.
   - Klicken Sie **Übernehmen und an Gerät senden**, um die Einstellungen zu speichern, ohne das Profil zu verlassen.
   - Klicken Sie **Speichern**, um die Einstellungen zu speichern und das Profil zu verlassen.

8. Weisen Sie das Profil den gewünschten Geräten / Geräteverzeichnissen zu. Siehe Wie kann ich IGEL UMS Profile zuweisen? (see page 379)

Neues Profil: Expertenmodus

> ⚠ Der **Expertenmodus** für Profile ist normalerweise NICHT erforderlich und sollte nur in Ausnahmefällen verwendet werden.

Die Auswahlmöglichkeiten im Fenster **Neues Profil > Expertenmodus** haben folgende Bedeutung:

Erbt Einstellungen von

Bestimmt, ob das neue Profil Einstellungen von einem bestehenden Profil oder Gerät übernimmt.

Aktiviere keine Einstellungen

Zunächst sind keine Parameter aktiv.

Aktiviere alle Einstellungen

Alle verfügbaren Parameter des Profils werden aktiviert. Beachten Sie, dass dadurch alle Einstellungen am Gerät mit einem Schloss-Symbol gesperrt sind. Ein Profil mit aktivierter Option **Aktiviere alle Einstellungen** verhindert die lokale Änderung von Einstellungen am Gerät. Diese Option ist nur dann sinnvoll, wenn Sie alle Einstellungen eines Geräts durch dieses Profil regeln lassen möchten.

Profile, die alle Parameter einer Firmware enthalten, belegen oft unnötig Platz in Datenbanken und Backup-Dateien. Daher sollten Sie diese Option nur dann verwenden, wenn es wirklich notwendig ist. In den allermeisten Fällen empfiehlt es sich, die Konfiguration eines Geräts über mehrere Profile mit spezifischen Konfigurationsteilen vorzunehmen.

Sitzungen überschreiben

Mit "Sitzungen" sind hier sowohl die Anwendungen, die man im Strukturbaum unter **Sitzungen** auswählen kann, wie auch alle anderen **freien Instanzen**, die man anlegen oder löschen kann, gemeint. Siehe Konfigurationsebenen (see page 369).

☑ Überschreibt die am Gerät definierten oder über andere Profile zugewiesenen freien Instanzen mit denen dieses Profils.

☐ Die im Profil definierten freien Instanzen werden zu den freien Instanzen hinzugefügt, die zuvor am Gerät oder durch Zuweisung von anderen Profilen definiert wurden. (Standard)

Die Option **Sitzungen überschreiben** stellt sicher, dass nur die freien Instanzen dieses Profils am Gerät angelegt werden. Freie Instanzen, die in anderen Profilen oder direkt in der Konfiguration des Geräts angelegt sind, werden unwirksam.

Sind einem Gerät (oder Shared Workplace-Benutzer) mehrere Profile mit aktivierter Option **Sitzungen überschreiben** zugewiesen, so wirkt das Profil mit der höchsten Priorität, d.h. nur die freien Instanzen dieses Profils stehen am Gerät zur Verfügung.
Ausnahme: Ist das Profil ein Standardprofil und ist dem Gerät (oder dem Benutzer) auch ein Priority Profil (see page 413) mit Sitzungseinstellungen zugewiesen, so werden die Einstellungen addiert: Das Gerät erhält alle Sitzungen des Standardprofils und des Priority Profils. Sitzungen in Priority Profilen können nur durch ein Priority Profil überschrieben werden.

IGEL Tech Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=Ml522x3qqn0

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=zeHiW4_uG0s&t=4s

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=h8EpnPNUmkg

Wie kann ich IGEL UMS Profile zuweisen?

In der IGEL Universal Management Suite (UMS) Konsole können Sie einem Gerät oder einem Geräteverzeichnis ein Profil zuweisen. Sie können einem Gerät oder einem Geräteverzeichnis ein Profil per Drag & Drop oder unter **Zugeordnete Objekte** in den Baumknoten **Profile** oder **Geräte** zuweisen.

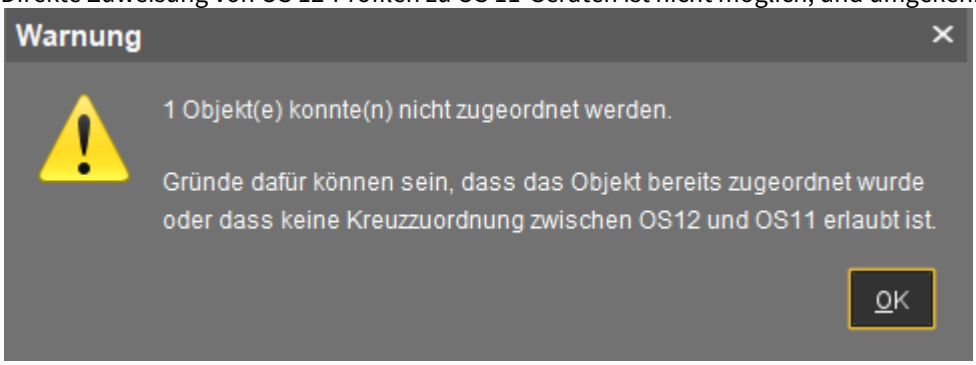
Direkte und indirekte Zuweisung von Objekten in der IGEL UMS
Objekte in der IGEL UMS können direkt oder indirekt zugeordnet werden:

- Direkt zugeordnete Objekte wurden einem einzelnen Gerät oder Ordner zugewiesen.
- Indirekt zugeordnete Objekte wurden über die Ordnerstruktur 'geerbt'.

Ob ein Profil direkt oder indirekt zugewiesen wird, beeinflusst die Priorität eines Profils, siehe Wirkungsordnung von Profilen (see page 399).
Beachten Sie das Folgende:

- Wenn Sie ein Profil einem Verzeichnis zuweisen, ist es **indirekt** jedem Gerät in diesem Verzeichnis zugewiesen, auch den Unterverzeichnissen.
- Wenn Sie ein Gerät nachträglich in dieses Verzeichnis verschieben, wirken sich die Verzeichnisprofile auch auf dieses Gerät aus.
- Wenn Sie einen Gerät aus diesem Verzeichnis entfernen, beeinflusst das Profil dieses Gerät nicht mehr und die lokalen Einstellungen des Geräts werden wieder hergestellt.

Direkte Zuweisung von OS 12-Profilen zu OS 11-Geräten ist nicht möglich, und umgekehrt:



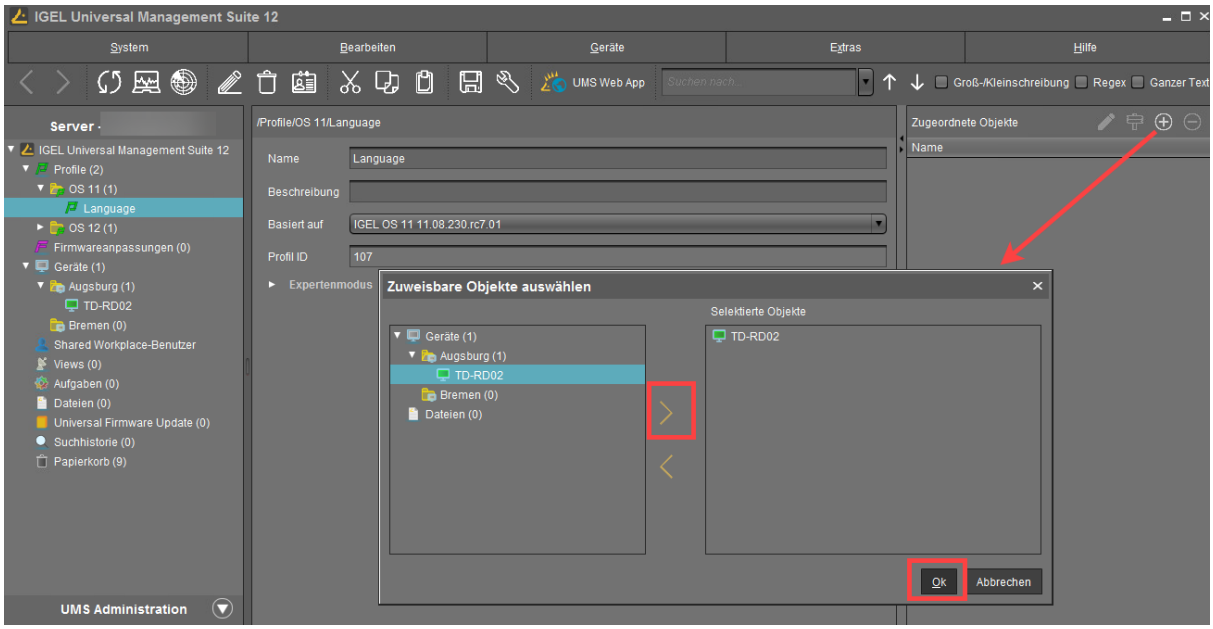
Wenn Sie ein OS 12-Profil einem OS 11-Gerät indirekt zuweisen, d.h. über eine Verzeichnisstruktur, wird das OS 12-Profil für das OS 11-Gerät NICHT berücksichtigt (und umgekehrt).

Ein Profil zuweisen: Vom Profil ausgehend

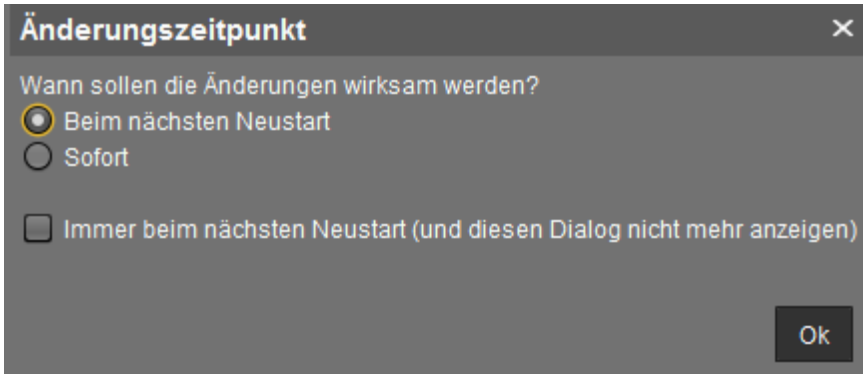
1. Gehen Sie in der UMS Konsole auf **Profile** und wählen Sie das gewünschte Profil aus.
2. Klicken Sie unter **Zugeordnete Objekte** auf ⊕.
   Das Fenster **Zuweisbare Objekte auswählen** öffnet sich.

3. Markieren Sie das gewünschte Gerät oder Geräteverzeichnis und klicken Sie  .

4. Klicken Sie **OK**.



5. Entscheiden Sie, ob die neuen Einstellungen sofort oder beim nächsten Start des Geräts wirksam werden sollen.



Denken Sie daran, dass Benutzer in ihrer Arbeit gestört werden können, wenn Sie die Änderungen sofort wirksam werden lassen.

> Geräte, die die Konfigurationsänderungen noch nicht erhalten haben, werden mit einem Ausrufezeichen markiert  .

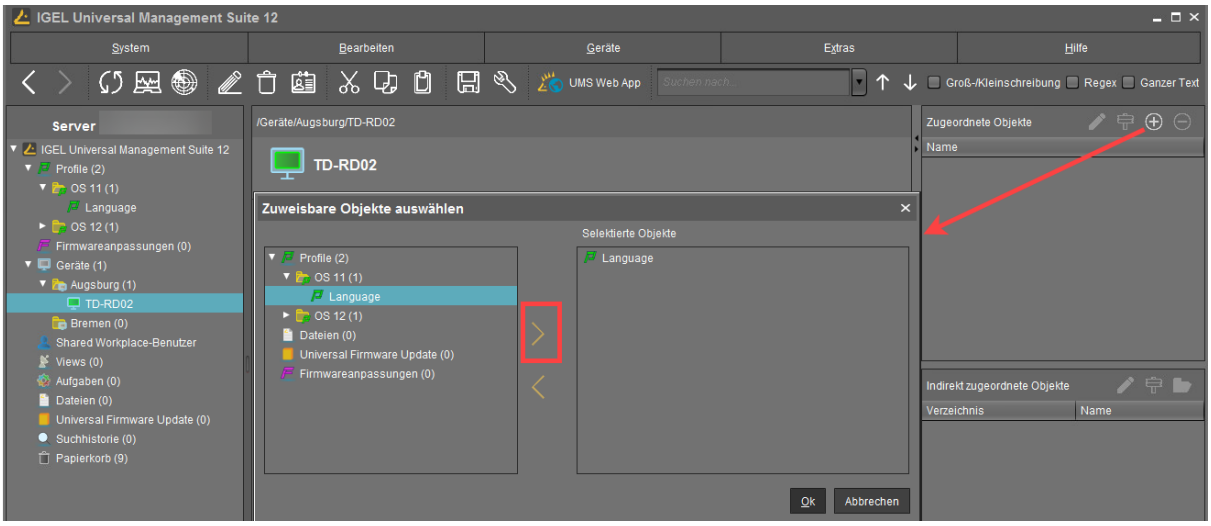
Ein Profil zuweisen: Vom Gerät / Geräteverzeichnis ausgehend

1. Gehen Sie in der UMS Konsole auf **Geräte** und wählen Sie das gewünschte Gerät oder Verzeichnis aus.

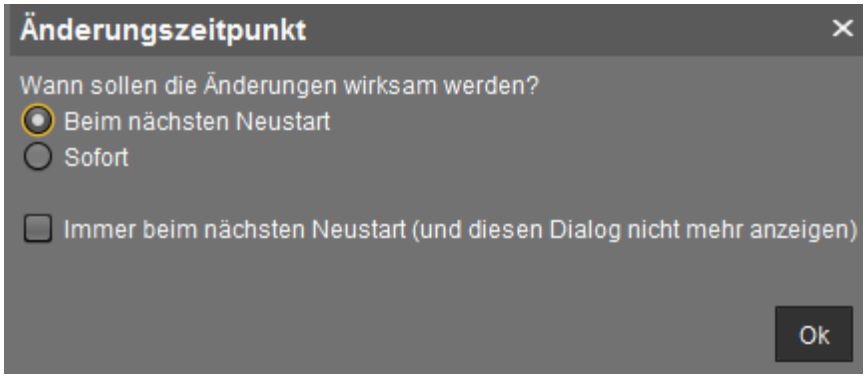
2. Klicken Sie unter **Zugeordnete Objekte** auf ⊕.
   Das Fenster **Zuweisbare Objekte auswählen** öffnet sich.

3. Markieren Sie das gewünschte Profil und klicken Sie ›.

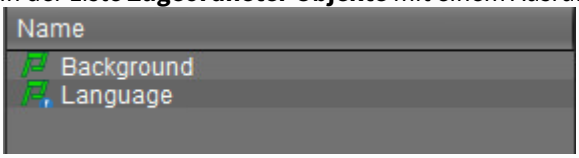
4. Klicken Sie **OK**.



5. Entscheiden Sie, ob die neuen Einstellungen sofort oder beim nächsten Start des Geräts wirksam werden sollen.



Denken Sie daran, dass Benutzer in ihrer Arbeit gestört werden können, wenn Sie die Änderungen sofort wirksam werden lassen.

> ⓘ Zugewiesene Profile mit noch nicht an die Geräte übertragenen Konfigurationsänderungen werden in der Liste **Zugeordneter Objekte** mit einem Ausrufezeichen markiert.
>
> 
>

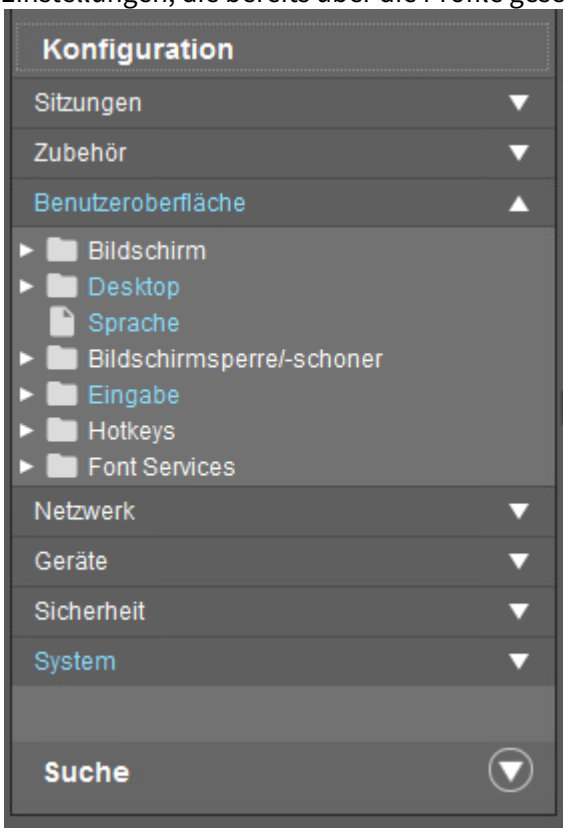
Profile in der IGEL UMS überprüfen

Wenn Sie in der IGEL Universal Management Suite (UMS) einem Gerät ein Profil zugewiesen haben, können Sie die Ergebnisse wie folgt überprüfen. In der IGEL UMS Web App können Sie dies wie unter Prüfen welche Profile die Parameter in der IGEL UMS Web App definieren (see page 861) beschrieben tun.

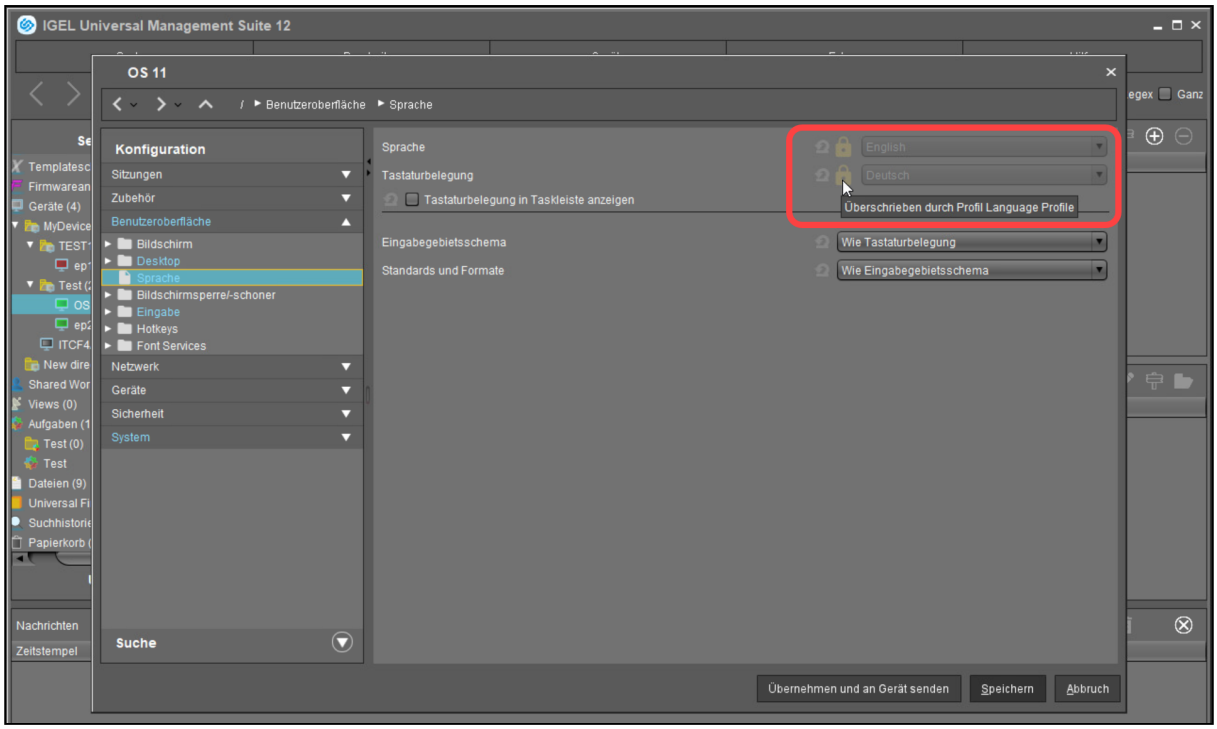
---

1. Gehen Sie in der UMS Konsole auf **Geräte** und wählen Sie das gewünschte Gerät aus.
2. Klicken Sie **[Kontextmenü des Geräts] > Konfiguration bearbeiten** oder **Bearbeiten > Konfiguration bearbeiten**.
   Oder doppelklicken Sie das Gerät.

   Die aktuelle Konfiguration des Geräts wird angezeigt. Blau markierte Pfade führen zu Einstellungen, die bereits über die Profile gesetzt sind.

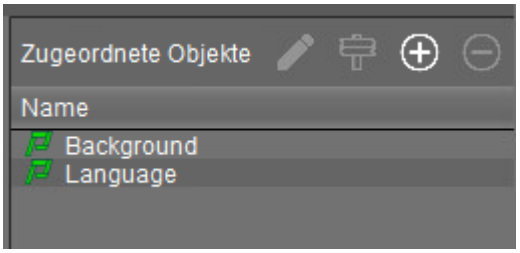


   Jede Einstellung, die durch ein Profil vorgegeben wird, ist durch ein Schloss-Symbol kenntlich gemacht. Der Wert, den Sie im Profil angegeben haben, wird angezeigt. Sie können die Einstellung hier nicht ändern.



3. Fahren Sie mit der Maus über das Schloss-Symbol.
   Ein Tooltip zeigt an, aus welchem Profil der Parameterwert gezogen wurde. Dies ist hilfreich, wenn Sie dem Gerät mehr als ein Profil zugewiesen haben. Wenn eine Einstellung in mehreren zugewiesenen Profilen aktiv ist, wird der Wert vom aktuellsten Profil genommen.

Im Bereich **Zugeordnete Objekte** können Sie zu einem zugewiesenen Objekt navigieren oder dessen Konfiguration bearbeiten.



- Wählen Sie ein Objekt aus und klicken Sie  , um das Objekt zu bearbeiten.
- Wählen Sie ein Objekt aus und klicken Sie  , um im Strukturbaum zu diesem Objekt zu navigieren.
- Doppelklicken Sie auf ein zugewiesenes Objekt, um direkt dorthin zu springen.

IGEL Tech Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=h8EpnPNUmkg

Profile in der IGEL UMS bearbeiten

In der IGEL Universal Management Suite (UMS) können Sie die existierenden Profile bearbeiten. Sie können sowohl die **Beschreibungsdaten** eines Profils als auch die **Profilkonfiguration** bearbeiten.

Menüpfad: **UMS Konsole > Profile**

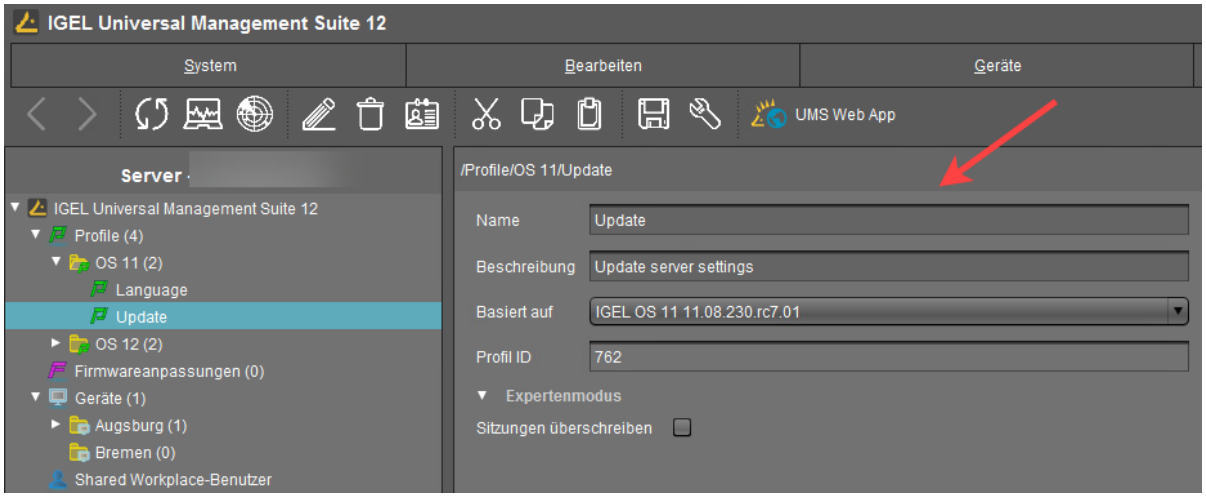
Beschreibungsdaten eines Profils bearbeiten

Beschreibungsdaten bestehen aus dem Namen des Profils, einem Beschreibungstext, der Firmwareversion, auf der dieses Profil basiert, und dem Überschreibungs-Flag für Sitzungen.

So bearbeiten Sie diese Einstellungen:

1. Wählen Sie unter **Profile** das gewünschte Profil aus.
2. Ändern Sie die Einstellungen nach Ihren Bedürfnissen.

   > Beachten Sie bei Änderungen der Firmwareversion unter **Basiert auf**, dass Profileinstellungen verloren gehen, wenn sie in der neuen Firmware nicht unterstützt werden.

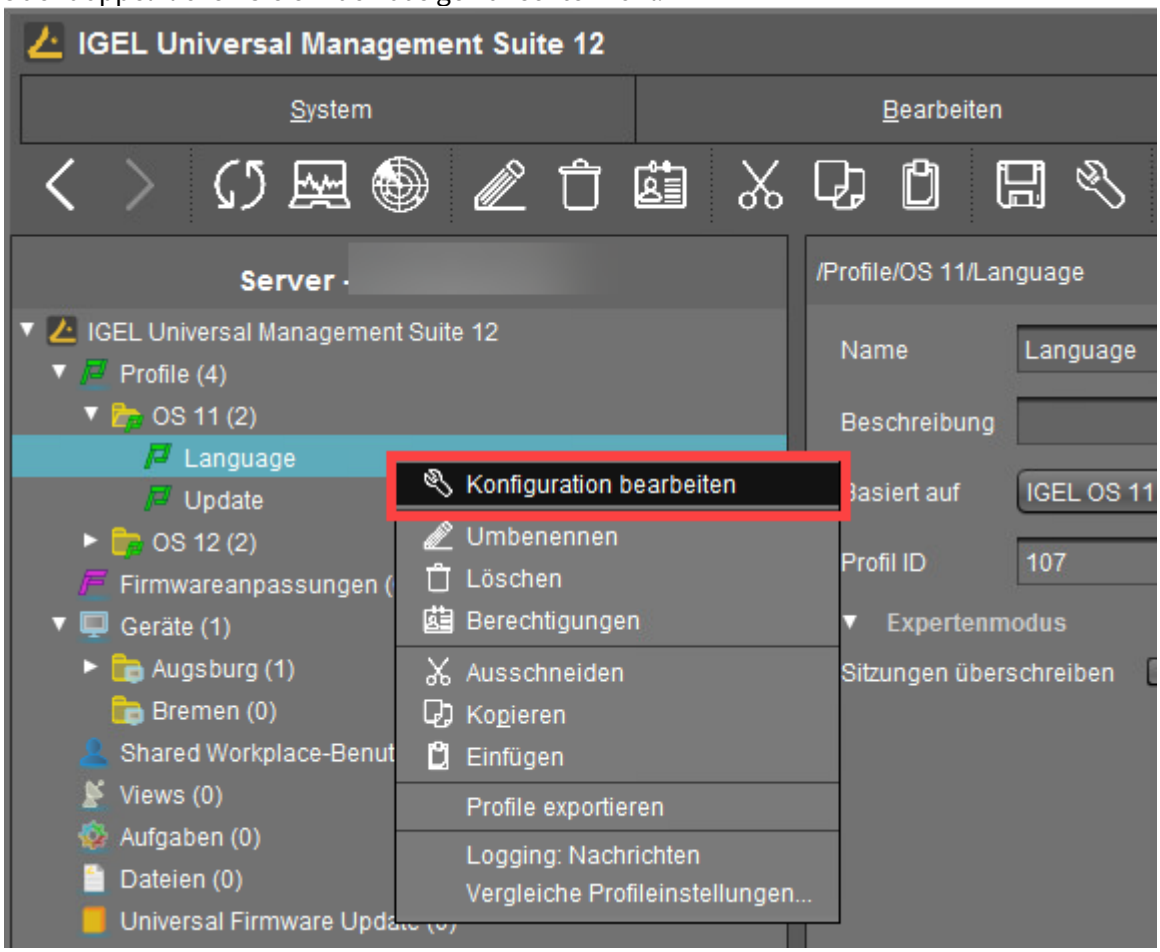
3. Um die Änderungen zu speichern, klicken Sie  oder **Bearbeiten > Beschreibungsdaten speichern**.

   Die Daten sind nun in der Datenbank aktualisiert.

Profilkonfiguration bearbeiten

So bearbeiten Sie die Profilkonfiguration:

1. Wählen Sie unter **Profile** das gewünschte Profil aus und klicken Sie **[Kontextmenü] > Konfiguration bearbeiten** oder **Bearbeiten > Konfiguration bearbeiten**.
   Oder doppelklicken Sie einfach das gewünschte Profil.



   Der Konfigurationsdialog öffnet sich.

   > ⓘ Blau markierte Pfade im Konfigurationsbaum führen zu Einstellungen, die bereits über das Profil gesetzt sind.

   > ⓘ Registry-Schlüssel (Einstellungen), die über ein Profil gesetzt sind, erscheinen ebenfalls farbig markiert. Die verwendeten Farben entsprechen denen zur Markierung von Pfaden im Konfigurationsbaum.

2. Um Einstellungen zu ändern, klicken Sie das Aktivierungssymbol vor dem Parameter, bis die gewünschte Funktion aktiv ist.

	Der Parameter ist inaktiv und wird nicht durch das Profil konfiguriert.
	Der Parameter ist aktiv und wird durch das Profil konfiguriert. Die Templateschlüssel sind inaktiv.
	Parameter auf Standardwert zurücksetzen.
Die folgenden Aktivierungssymbole werden nur angezeigt, wenn Templateprofile aktiviert sind (siehe Templateprofile in der IGEL UMS (see page 416)):	
	Der Parameter ist aktiv und wird durch das Profil konfiguriert. Die Templateschlüssel sind aktiv.
	Der Parameter ist aktiv und wird durch das Profil konfiguriert. Der Parameter wird aus einem Templateschlüssel bezogen.

3. Speichern Sie die Änderungen.

4. Bestimmen Sie, wann die Änderungen wirksam werden sollen – sofort oder beim nächsten Start des Geräts.

Profilzuweisung vom Gerät entfernen

So können Sie die Zuordnung zwischen Profilen und Objekten aufheben:

Vom Profil ausgehend

1. Markieren Sie ein Profil im Navigationsbaum.
2. Wählen Sie im Fensterbereich **Zugeordnete Objekte** ein Objekt.
3. Klicken Sie ⊖ .

Vom Gerät ausgehend

1. Markieren Sie ein Gerät im Navigationsbaum.
2. Wählen Sie im Fensterbereich **Zugeordnete Objekte** ein zugewiesenes Profil aus der Liste.
3. Klicken Sie ⊖ .

Dieses Profil hat nun keine Auswirkungen mehr auf das entsprechende Objekt. Der überschriebene Wert der Einstellungen wird auf den Wert zurückgesetzt, der vor Zuweisung des Profils gültig war.

> ⓘ Es können nur direkt zugeordnete Profile entfernt werden. Indirekt zugeordnete Profile können nur dort entfernt werden, wo sie 'direkt' zugeordnet sind, also am Ordner.

Profile löschen

Wenn Sie ein Profil löschen möchten, wählen Sie dieses im UMS Navigationsbaum aus und führen Sie eine der folgenden Aktionen durch:

- Klicken Sie in der Symbolleiste auf  **Löschen.**
- Drücken Sie die [Entf]-Taste auf Ihrer Tastatur
- Klicken Sie mit der rechten Maustaste auf das Profil, und wählen Sie aus dem Kontextmenü die Option **Löschen**.

Gleiches gilt auch für Verzeichnisse. Diese werden mitsamt allen Unterverzeichnissen und Profilen gelöscht.

> Wenn Sie ein Profil löschen, werden auch alle Zuweisungen des Profils entfernt. Die Konfiguration des Profils wirkt nicht mehr auf die Geräteeinstellungen. Außerdem werden alle Einstellungen des Profils aus der Datenbank gelöscht.

Wenn Sie den Papierkorb aktiviert haben, dann wird das gelöschte Profil dort abgelegt und kann bei Bedarf wiederhergestellt werden.

Profile exportieren und importieren

In der IGEL Universal Management Suite (UMS) können Profile samt ihrer Verzeichnisstruktur aus der Datenbank exportiert werden. Dies kann für Backupzwecke oder zum Importieren von Profildaten aus einer UMS Installation in eine andere hilfreich sein.

Alternativ können auch Einstellungen von Geräten als Profile importiert werden; siehe Geräte als Profile importieren (see page 473).

> In der UMS Konsole können nur OS 11-Profile exportiert oder importiert werden. Wenn Sie OS 12-Profile exportieren / importieren möchten, siehe Profile in der IGEL UMS Web App exportieren und importieren (see page 852).

Profil und Firmwareinformationen exportieren

So exportieren Sie ein einzelnes Profil:

1. Klicken Sie mit der rechten Maustaste auf das Profil.
2. Wählen Sie den Befehl **Exportiere Profile.**

So exportieren Sie mehrere Profile in eine Datei (ZIP-Archiv):

1. Markieren Sie die gewünschten Profile mit den Tasten [Strg] bzw. [Umschalt].
2. Wählen Sie **System > Exportieren > Profil exportieren.**
   Das Fenster **Profile exportieren** öffnet sich.

3. Wählen Sie die gewünschten Profile in der Spalte **Aufnehmen** aus.
4. Bestätigen Sie mit **OK**.
5. Wählen Sie die Zieldatei aus.

Die Firmwareinformationen lassen sich gemeinsam mit den Profildaten in ein Archiv exportieren, dies erlaubt den Import auch in eine *UMS* Installation ohne passende registrierte Firmware. Diese kann nun zusammen mit dem Profil importiert werden.

Die Profile werden in das XML-Format konvertiert. Achten Sie darauf, diese Dateien nicht zu veröffentlichen, wenn die Quellprofile Passwörter oder andere vertrauliche Daten enthalten!

Profil und Firmwareinformationen importieren

So importieren Sie ein einzelnes Profil:

1. Klicken Sie in der UMS Konsole **System > Importieren > Profile importieren**.
2. Wählen Sie die `XML` -Datei bzw. das Archiv mit Ihrem/Ihren Profile/n aus.
   Das Dialogfenster **Profile importieren** wird geöffnet. Hier werden der Name und die Firmwareversion jeder Profilkonfiguration angezeigt, die in der von Ihnen ausgewählten Datei enthalten ist.
3. Wenn Sie ein Profil vom Import ausschließen wollen, deaktivieren Sie das zugehörige Kontrollkästchen.

   > Beim Import lässt sich der ursprüngliche Verzeichnispfad des Profils beibehalten oder aber das Profil wird im Hauptverzeichnis abgelegt.

   Ein Dialogfenster zeigt an, ob alle gewählten Profile importiert wurden.
   Falls das Profil eine Firmwareinformation benötigt, die bisher nicht in der Datenbank vorhanden ist, wird diese automatisch zusammen mit dem entsprechenden Profil aus dem Archiv importiert, vorausgesetzt, es wurde beim Export der Haken **Firmwares mit exportieren** aktiviert!

- Profile mit unbekannter Firmware importieren (see page 393)

Profile mit unbekannter Firmware importieren

Ein Profil, dessen zugrundeliegende Firmwareinformation weder in der Datenbank vorhanden, noch in der Importdatei enthalten ist, kann nicht ohne Anpassungen importiert werden. Es ist in der Importansicht rot markiert.

Solche Profile können Parametereinstellungen enthalten, die in keiner der registrierten Firmwareversionen enthalten sind.

So importieren Sie Profile, die eine unbekannte Firmware referenzieren:

1. Klicken Sie auf das rot markierte Firmwarefeld.
2. Wählen Sie eine möglichst verwandte Firmwareversion aus, die dem System bekannt ist.
3. Importieren Sie das Profil.

Wenn eine **bekannte** Firmware gewählt wird, findet eine implizite Konvertierung der Profilinformationen statt. Dies hat normalerweise kaum Auswirkungen auf die Profileinstellungen, wenn Sie eine ähnliche Firmware oder eine neuere Version des gleichen Modells auswählen. Parameter, die in der neuen Firmware nicht definiert sind, gehen dabei aber verloren.

Profile in der IGEL UMS kopieren

In der IGEL Universal Management Suite (UMS) können Sie ein Profil kopieren und in ein beliebiges Profilverzeichnis einfügen.

> Das Kopieren und Einfügen ist auch zwischen Standardprofilverzeichnissen und Priority Profil-Verzeichnissen möglich. Wenn Sie ein Standardprofil kopieren und in ein Priority Profil-Verzeichnis einfügen, so wird die Kopie des Standardprofils als Priority Profil definiert. Wenn Sie ein Priority Profil kopieren und in ein Standardprofilverzeichnis einfügen, so wird die Kopie als Standardprofil definiert. Informationen zu Priority Profilen finden Sie unter Priority Profile in der IGEL UMS (see page 413).

Menüpfad: **UMS Konsole > Profile**

> Es ist derzeit nicht möglich, IGEL OS 12-Profile zu kopieren.

So kopieren Sie ein Profil:

1. Klicken Sie in der **UMS Konsole > Profile** das Profil, das Sie kopieren wollen.
2. Öffnen Sie das Kontextmenü des Profils und wählen Sie **Kopieren**.
3. Klicken Sie das Profilverzeichnis, in das Sie die Kopie des Profils einfügen wollen. Dies kann auch das Verzeichnis des ursprünglichen Profils sein.
4. Öffnen Sie das Kontextmenü des Verzeichnisses und wählen Sie **Einfügen**.
   Ein neues Profil wird angelegt, das den gleichen Namen sowie die gleichen Einstellungen hat wie das ursprüngliche Profil. Das neue Profil ist noch keinem Gerät zugewiesen, unabhängig von den Zuweisungen des ursprünglichen Profils.

Profilverzeichnisse in der IGEL UMS kopieren

In der IGEL Universal Management Suite (UMS) können Sie ein Profilverzeichnis kopieren und in ein beliebiges Verzeichnis einfügen.

> Das Kopieren und Einfügen ist auch zwischen Standardprofilverzeichnissen und Priority Profil-Verzeichnissen möglich. Wenn Sie ein Standardprofilverzeichnis kopieren und in ein Priority Profil-Verzeichnis einfügen, so werden die dabei angelegten Kopien der Standardprofile als Priority Profile definiert. Wenn Sie ein Priority Profil-Verzeichnis kopieren und in ein Standardprofilverzeichnis einfügen, so werden die dabei angelegten Kopien der Priority Profile als Standardprofile definiert. Informationen zu Priority Profilen finden Sie unter Priority Profile in der IGEL UMS (see page 413).

Menüpfad: **UMS Konsole > Profile**

So kopieren Sie ein Profilverzeichnis:

1. Klicken Sie das Profilverzeichnis, das Sie kopieren wollen.
2. Öffnen Sie das Kontextmenü des Profilverzeichnisses und wählen Sie **Kopieren**.
3. Klicken Sie das Verzeichnis, in das Sie die Kopie des Profilverzeichnisses einfügen wollen. Dies kann auch das Verzeichnis sein, indem sich das ursprüngliche Profilverzeichnis befindet.
4. Öffnen Sie das Kontextmenü des Verzeichnisses und wählen Sie **Einfügen**.

Ein neues Profilverzeichnis wird angelegt, das den gleichen Namen hat wie das ursprüngliche Profilverzeichnis. Das neue Profilverzeichnis enthält neu angelegte Kopien der im ursprünglichen Profilverzeichnis enthaltenen Profile sowie Kopien der Unterverzeichnisse. Die Kopien der Profile sind noch keinem Gerät zugewiesen, unabhängig von den Zuweisungen der ursprünglichen Profile.

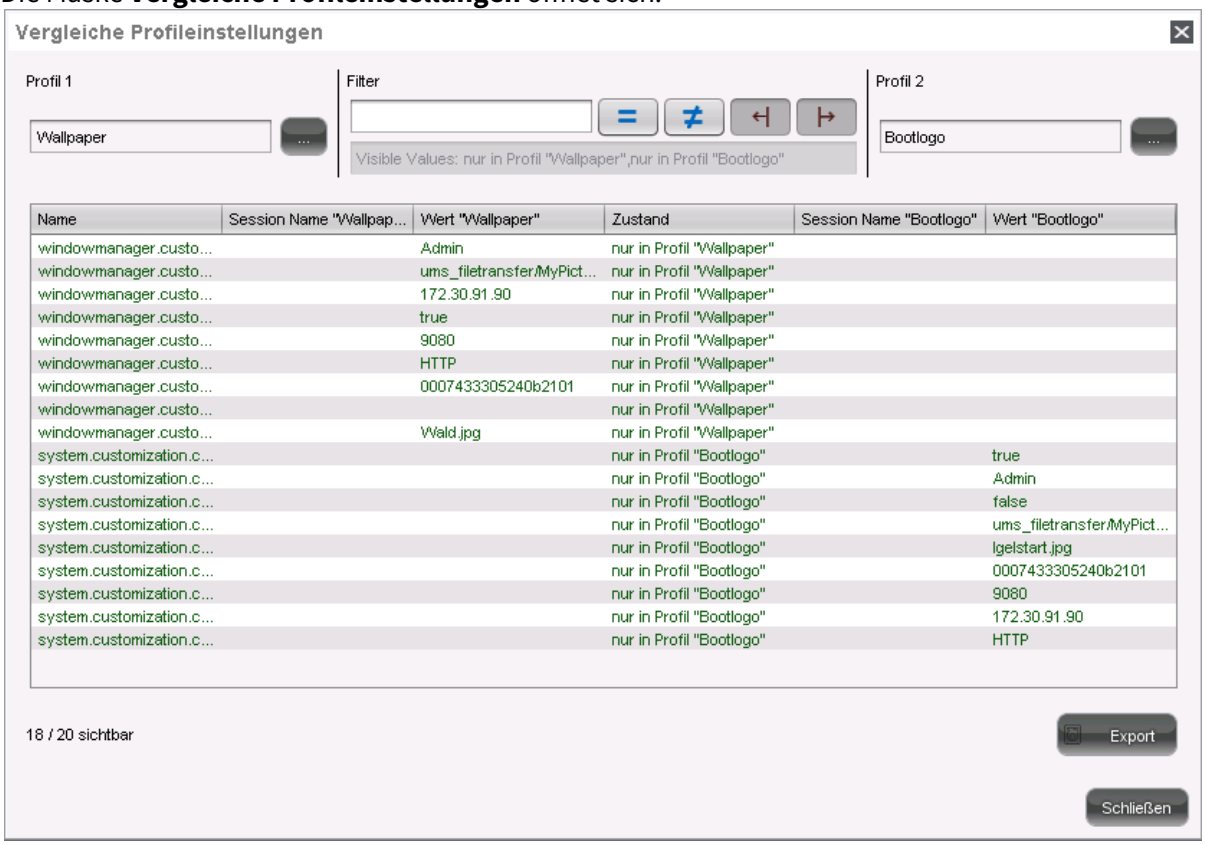
Profile in der IGEL UMS vergleichen

In der IGEL Universal Management Suite können Sie eine Funktion verwenden, über die Sie auf einfache Weise Profile miteinander vergleichen können.

Menüpfad: **UMS Konsole > Profile**

So vergleichen Sie zwei Profile:

1. Markieren Sie mit Hilfe der [Strg]-Taste zwei Profile.
2. Klicken Sie mit der rechten Maustaste auf eins dieser Profile.
3. Wählen Sie aus dem Kontextmenü **Vergleiche Profileinstellungen...** .
   Die Maske **Vergleiche Profileinstellungen** öffnet sich.



In der Standardansicht sind alle Einstellungen, die in den beiden Profilen vorgenommen wurden, untereinander aufgelistet. Über folgende Schaltflächen können Sie bestimmte Vergleichsoperatoren einsetzen:

		Einstellungen, die in beiden Profilen gleich sind, werden ein- oder ausgeblendet.
		Einstellungen, die sich in den Profilen unterscheiden, werden ein- oder ausgeblendet.
		Einstellungen, die nur in Profil 1 vorhanden sind, werden ein- oder ausgeblendet.
		Einstellungen, die nur in Profil 2 vorhanden sind, werden ein- oder ausgeblendet.

- Klicken Sie auf eine dieser Schaltflächen, um den entsprechenden Vergleichsoperator zu deaktivieren.
- Klicken Sie erneut darauf, um den Operator wieder zu aktivieren.

inaktiv aktiv

- Aktivieren oder deaktivieren Sie mehrere Vergleichsoperatoren.
- Klicken Sie **Export**, um sich die Vergleichsliste als csv-, html- oder xml-Datei lokal zu speichern.

Priorisierung von Profilen in der IGEL UMS

In der IGEL Universal Management Suite (UMS) können Profile den Geräten direkt oder indirekt über Verzeichnisse zugewiesen werden. Ein Gerät kann seine Einstellungen von mehreren direkt oder indirekt zugewiesenen Profilen bekommen. Bei der Zuweisung überschreiben die Profileinstellungen die direkt am Gerät vorgenommenen Einstellungen.

Wenn Sie IGEL Shared Workplace benutzen, haben Sie die Möglichkeit, Profile Benutzern zuzuordnen. Profile, die Benutzern zugewiesen sind, haben mehr Gewicht als die, die Geräten zugewiesen sind. Siehe dazu Wirkungsordnung der Profile in IGEL Shared Workplace (see page 402).

Die Einrichtung und Konfiguration von Profilen ist unter Profile verwenden (see page 371) beschrieben. In diesem Kapitel geht es primär um die Priorisierung – welches Profil wann welches übersteuert.

Wirkungsordnung

Im Folgenden wird die Priorität von Profilen über eine stilisierte LED-Anzeige symbolisiert. Je mehr rote Lämpchen leuchten, desto höher die Priorität des Profils.

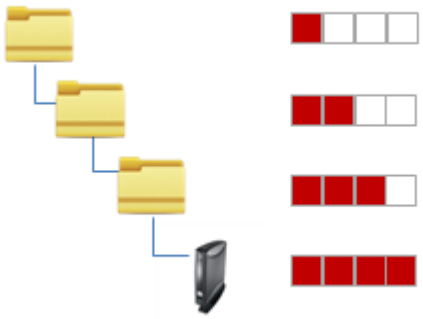
Wirkungsordnung von Profilen

Damit man die Wirkung der unterschiedlichen Profiltypen steuern kann, muss man die Rangfolge verstehen. Einem Gerät können unterschiedliche Profile zugewiesen sein, die wie Schablonen übereinander liegen. Was passiert, wenn zwei Profile den Wert einer Einstellung unterschiedlich vorgeben? Welche Vorgabe wirkt stärker?

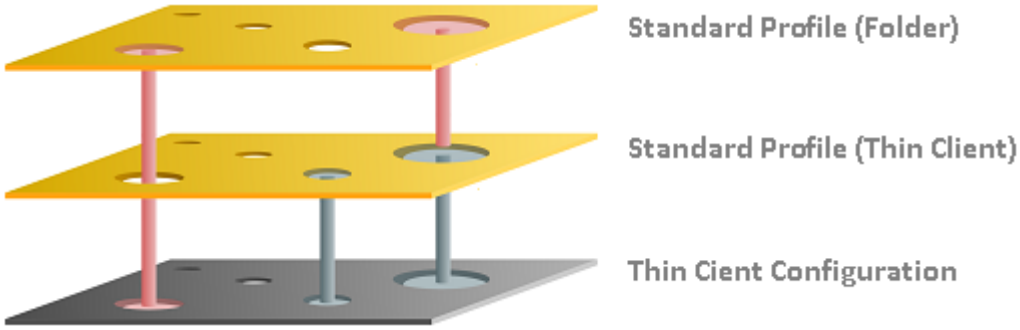
> Vermeiden Sie konkurrierende Einstellungen in mehreren Profilen. Richten Sie nach Möglichkeit pro Einstellung ein Profil ein, z.B. ein Profil für Spracheinstellungen, ein Profil für eine Linkshändermaus etc.

Für konkurrierende Einstellungen verschiedener Profile gelten folgende Regeln:

Regel: Je näher das Standardprofil im Verzeichnisbaum dem Gerät ist, umso höher ist seine Priorität.



Die Prioritätenregelung spielt nur dann eine Rolle, wenn der gleiche Parameterwert von zwei Profilen unterschiedlich belegt ist. Die folgende Grafik zeigt, dass es in beiden Profilen Wertevorgaben gibt, die auf das Gerät wirken. Nur der eine Parameter rechts ist von beiden Pofilen gesetzt. Hier hat der Wert des unteren Profils die Priorität, weil es näher am Gerät ist.



Regel: Für den Fall, dass gleiche Einstellungen mehrfach vorgegeben werden, übersteuern die Profile mit höherer Priorität andere Profile. Einstellungen, die nur in einem Profil vergeben sind, ändern ihre Wirkung nicht.

Siehe folgendes Beispiel (see page 401).

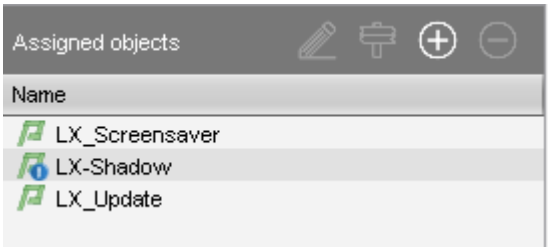
Regel: Wenn mehrere Profile gleichrangig zugewiesen sind, hat das neuere Profil, mit der höheren Profil-ID, Priorität.

> Um die ID eines Profils auszulesen, zeigen Sie mit dem Mauspfeil auf ein Profil in der Liste der zugewiesenen Profile. Es wird ein Tooltip mit der Profil-ID angezeigt.

Regel: Die Prioritätenregelung gilt nur für allgemeine Einstellungen. Wenn mehrere Sessions eingerichtet sind, werden sie nicht übersteuert, sondern existieren parallel nebeneinander, denn freie Instanzen werden addiert.

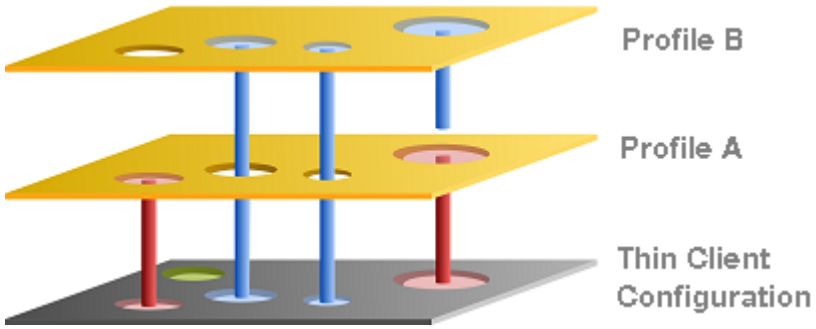
Die Listen der direkt oder indirekt zugewiesenen Profile sind entsprechend der Prioritätenfolge geordnet. Innerhalb einer Verzeichnisebene hat also das Profil weiter oben in der Liste die höhere Priorität.

In diesem Beispiel hat das Profil "Screensaver" die höchste Priorität:



Beispiel Standardprofile

Wir erstellen in der IGEL Universal Management Suite (UMS) drei Profile, die wir direkt und indirekt einem Gerät zuweisen:



- **Gerätekonfiguration**: Direkt am Gerät legen Sie die Mauseinstellungen fest. Hier ist (grün) die Linkshändermaus vorgegeben.
- **Profil A**: Sie weisen dem Gerät ein Sprachprofil zu, in dem (rot) die Sprache und die Tastaturbelegung auf Deutsch gesetzt ist.
- **Profil B**: Sie weisen einem darüber liegenden Verzeichnis ein Profil mit Bildschirmkonfiguration zu. Hier werden die Auflösung und die Einstellungen für zwei Bildschirme vorgegeben und die Sprache wird auf Englisch eingestellt (blau).

Die Einstellungen, die am Gerät ankommen, sind:

- grün: Linkshändermaus (Gerätekonfiguration)
- rot: Sprache und Tastatur Deutsch (Profil A)
- blau: Auflösung und Einstellung für zwei Bildschirme (Profil B)

Die Spracheinstellung "Englisch" aus Profil B hat am Gerät keine Wirkung, da Profil A den Sprachparameter auf Deutsch gesetzt hat. Da Profil A näher am Gerät ist, hat es Priorität.

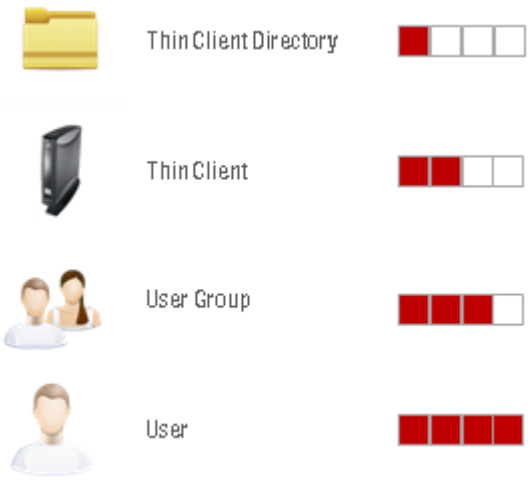
Wirkungsordnung der Profile in IGEL Shared Workplace

In IGEL Shared Workplace (see page 951) haben Sie die Möglichkeit, Profile für die Konfiguration von Benutzereinstellungen einzusetzen. Für nähere Informationen siehe IGEL Shared Workplace - Benutzerprofil zuweisen (see page 955).

> ⚠ Templateprofile und Templateschlüssel (see page 416) können nicht verwendet werden, wenn Shared Workplace benutzt wird.

Regel: Profile, die Benutzern zugewiesen sind, haben höhere Priorität als die, die Geräten zugewiesen sind. Dies gilt für Standardprofile und Priority Profile.

Wenn Sie mehrere Profile vergeben, kann es sein, dass bestimmte Benutzer- oder Clienteinstellungen mehrmals belegt sind. In diesem Fall gilt folgende **Priorisierung der Standardprofile**:



Höhere Priorität	als...
benutzerspezifische Profile	gerätespezifische Profile
näher am Benutzer/Gerät	weiter weg vom Benutzer/Gerät

Höhere Priorität	als...
Primäre Gruppen	sonstige Gruppen

sonstige Gruppen	Organizational Unit

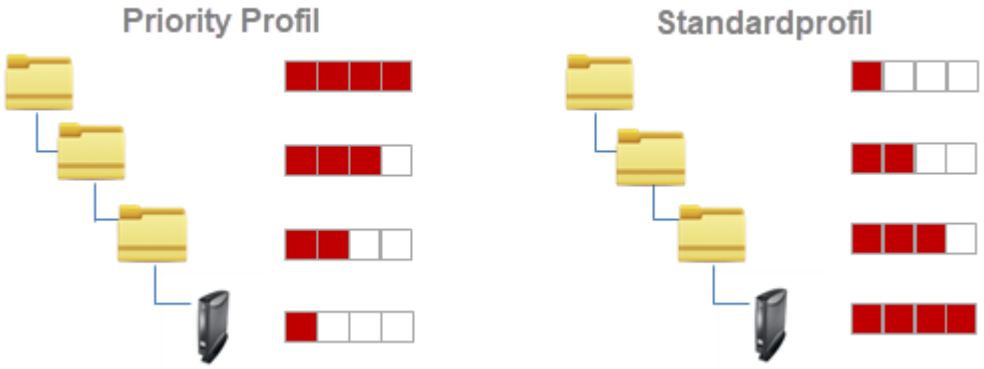
Regel: Profile, die einem Objekt zugewiesen sind, werden in absteigender Reihenfolge nach der Profil-ID priorisiert (höchste ID=höchste Priorität).

Regel: Gruppen innerhalb einer Ebene werden in alphabetischer Reihenfolge priorisiert.

Wirkungsordnung von Priority Profilen

Priority Profile erlauben eine flexiblere Gestaltung der Zugriffsrechte innerhalb der IGEL Universal Management Suite (UMS), indem sie Einstellungen von Standardprofilen übersteuern können und eigene Berechtigungen besitzen.

Priority Profile sind hinsichtlich ihrer Priorisierung untereinander **umgekehrt** gestaffelt als die Standardprofile. Das heißt, eine konkurrierende Profileinstellung ist umso höher priorisiert, je weiter das Profil vom Objekt entfernt ist:

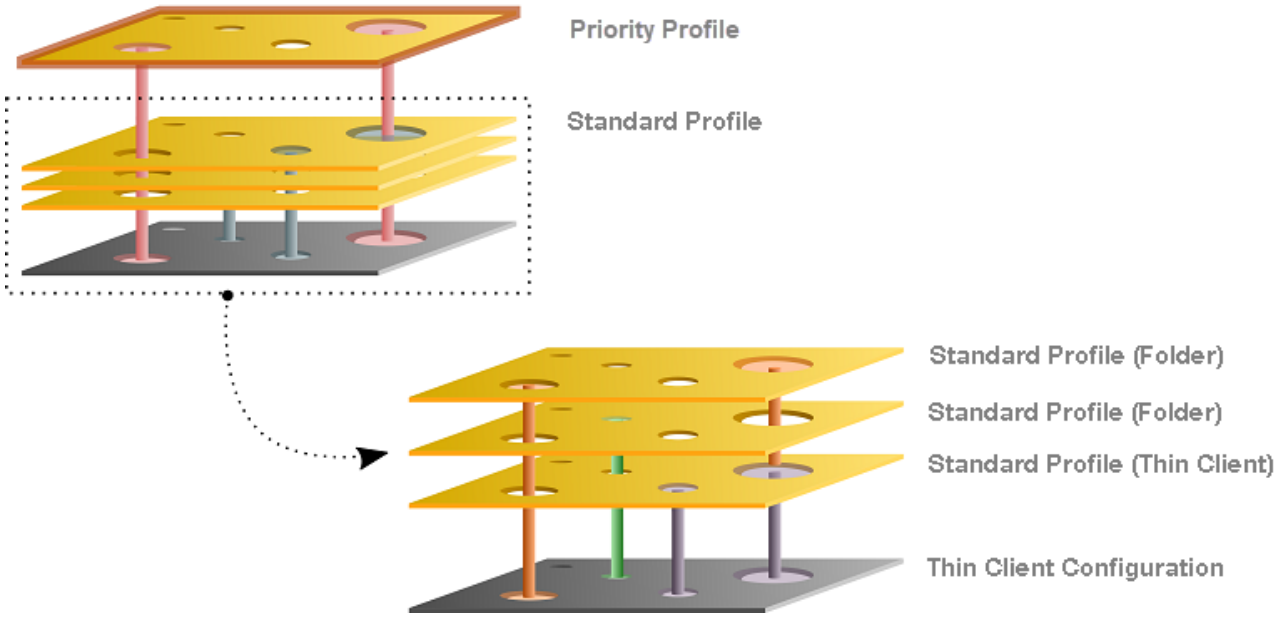


Bei Priority Profilen gilt:

Höhere Priorität	als...
weiter weg vom Gerät	näher am Gerät
übergeordnetes Verzeichnis	Unterverzeichnis

Regel: Priority Profile übersteuern alle Standardprofile.

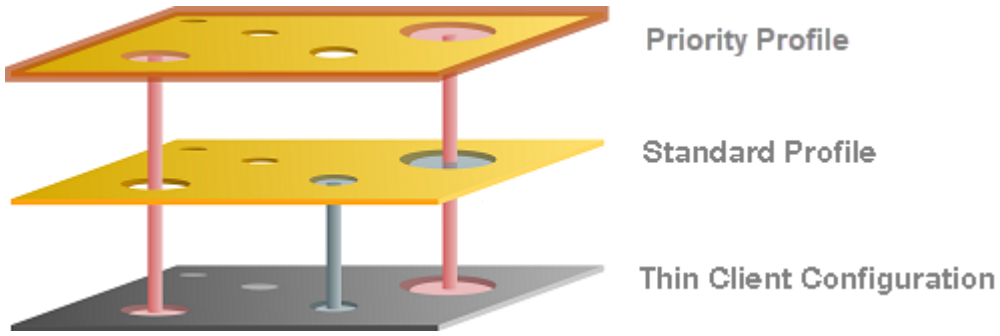
Die folgende Grafik zeigt, dass bei Vorbelegung des gleichen Parameters – oben rechts – die Einstellung des Priority Profils die der Standardprofile übersteuert. Einstellungen, die nicht doppelt belegt sind, wirken uneingeschränkt.



- Beispiel Priority Profile (see page 406)
- Beispiel Priority Profile und verschiedene Standardprofile (see page 407)
- Priority Profile in IGEL Shared Workplace (see page 408)

Beispiel Priority Profile

Wir erstellen in der IGEL Universal Management Suite (UMS) ein Standardprofil und ein Priority Profil, die wir einem Gerät zuweisen.



- **Standardprofil**: Sie weisen dem Gerät ein Standardprofil zu, in dem (grau) die Sprache und die Tastaturbelegung auf Deutsch gesetzt ist.
- **Priority Profil**: Sie weisen einem darüber liegenden Verzeichnis ein Priority Profil zu. Hier wird das Hintergrundbild vorgegeben und die Sprache wird auf Englisch eingestellt (rot).

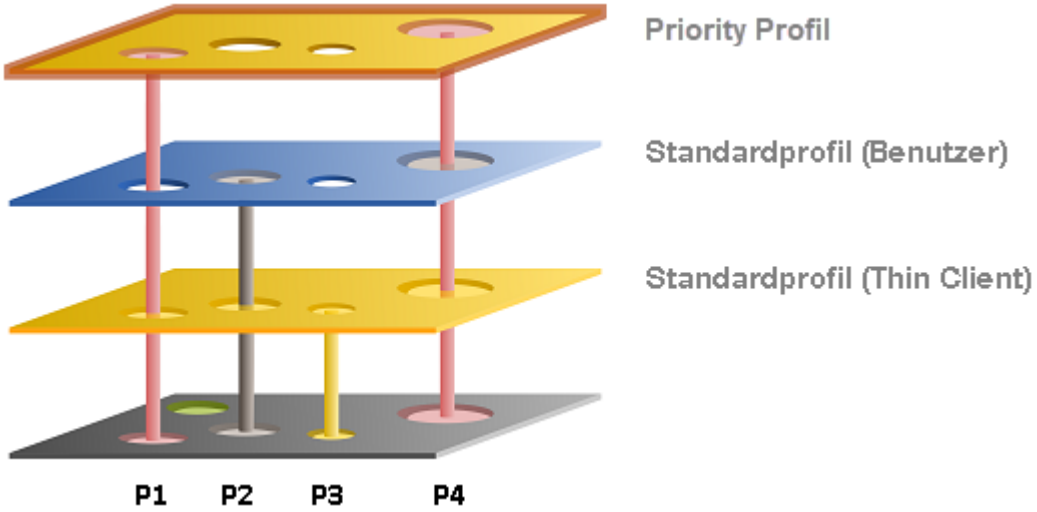
Die Einstellungen, die am Gerät ankommen, sind:

- grau: Tastatur Deutsch (Standardprofil)
- rot: Hintergrundbild und Spracheinstellung Englisch (Priority Profil)

Die Spracheinstellung "Deutsch" aus dem Standardprofil hat am Gerät keine Wirkung, da das Priority Profil den Sprachparameter auf Englisch gesetzt hat. Das Priority Profil überschreibt bei gleichen Parametereinstellungen die Werte von Standardprofilen.

Beispiel Priority Profile und verschiedene Standardprofile

Wir erstellen in der IGEL Universal Management Suite (UMS) ein Priority Profil, ein benutzerspezifisches Standardprofil und ein gerätespezifisches Standardprofil.



- **Standardprofil (Gerät)**: Sie weisen dem Gerät ein Standardprofil zu, mit dem Sie die Mauseinstellungen festlegen. Hier ist die Linkshändermaus (**P2**), die Geschwindigkeit des Mauszeigers (**P4**) auf langsam, das Doppelklick-Intervall (**P1**) auf langsam und die Tastaturbelegung auf Deutsch (**P3**) vorgegeben.
- **Standardprofil (Benutzer)**: Sie weisen einem darüber liegenden Verzeichnis ein benutzerspezifisches Standardprofil zu, in dem die Rechtshändermaus (**P2**) und die Mausgeschwindigkeit (**P4**) auf schnell gesetzt ist.
- **Priority Profil**: Sie weisen einem darüber liegenden Verzeichnis ein Priority Profil zu. Hier wird die Mauszeiger-Geschwindigkeit (**P4**) und das Doppelklick-Intervall (**P1**) auf mittel gesetzt.

Die Einstellungen, die am Gerät ankommen, sind:

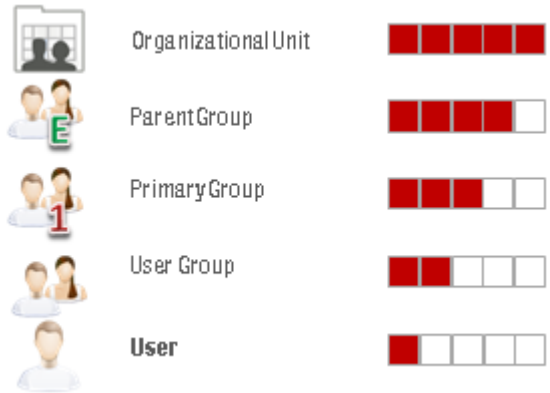
- gelb: (**P3**) Tastaturbelegung Deutsch (Standardprofil Gerät)
- grau: (**P2**) Rechtshändermaus (Standardprofil Benutzer)
- rot: (**P4**, **P1**) Mausgeschwindigkeit und Doppelklick-Intervall mittel (Priority Profil)

Priority Profile in IGEL Shared Workplace

Profile, die Benutzern zugewiesen sind, haben höhere Priorität als Profile, die Geräten zugewiesen sind. Bei den Priority Profilen ist nicht der einzelne Client oder Benutzer priorisiert, sondern die jeweilige Gruppe. Das heißt:

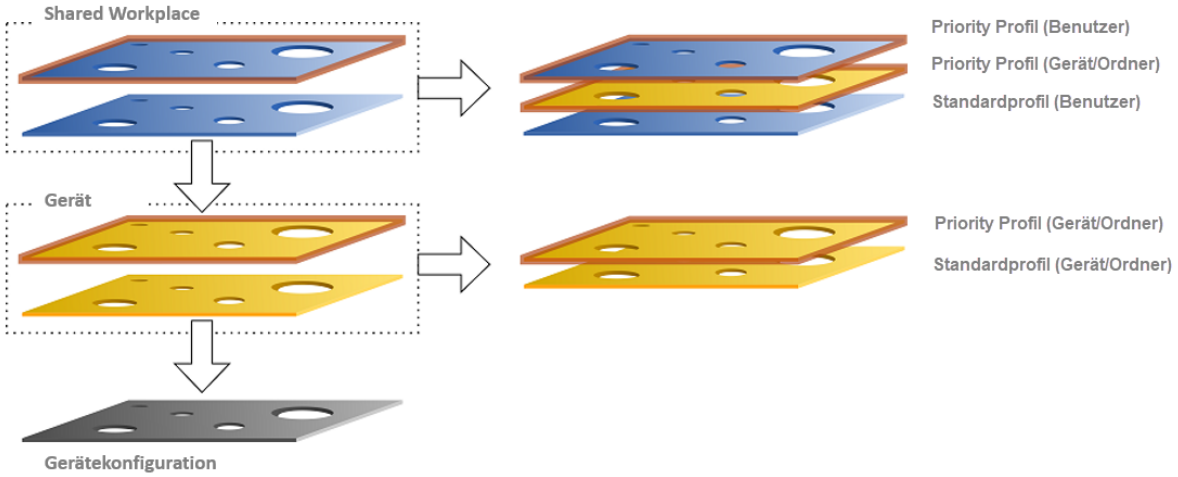
Regel: Priority Profile, die Benutzergruppen zugewiesen sind, haben höhere Priorität als die, die einzelnen Benutzern zugewiesen sind. Diese haben höhere Priorität als Priority Profile, die Geräteverzeichnissen zugewiesen sind. Die niedrigste Priorität haben Priority Profile, die einem einzelnen Gerät zugewiesen sind.

Höhere Priorität	als...
benutzerspezifische Profile	gerätespezifische Profile
weiter weg vom Benutzer/Gerät	näher am Benutzer/Gerät



Höhere Priorität	als...
Organizational Unit	sonstige Gruppen
sonstige Gruppen	Primäre Gruppe

Wirkungsordnung von allen Profilen



Parameter der Profilebene (Gerät und Shared Workplace)

- werden von Profilen oder Priority Profilen vorgegeben,
- sind ausschließlich über die UMS konfigurierbar,
- überschreiben Parameterwerte, die direkt am Gerät konfiguriert wurden,
- wirken durch Zuweisung an Gerät oder Verzeichnisse,
- sind einzeln aktivierbar.

Parameter der Gerätekonfiguration

- sind direkt am Gerät oder über die UMS konfigurierbar,
- enthalten immer ALLE Parameter,
- existieren IMMER, auch ohne UMS.

Zusammenfassung - Priorisierung von IGEL UMS Profilen

Nachfolgende Übersicht fasst alle Regeln rund um die Priorisierung von Profilen in der IGEL Universal Management Suite (UMS) zusammen:

A - Grundregel

- Für den Fall, das gleiche Einstellungen mehrfach vorgegeben werden, übersteuern die Profile mit höherer Priorität andere Profile. Siehe Grafik im Beispiel (see page 401).
- Einstellungen, die nur in einem Profil vergeben sind, werden nicht übersteuert.
- Die Prioritätenregelung gilt nur für allgemeine Einstellungen und feste Instanzen. Wenn z.B. mehrere freie Instanzen (see page 369) eingerichtet sind, werden sie nicht übersteuert, sondern existieren parallel nebeneinander.
- Wenn mehrere Profile gleichrangig zugewiesen sind, hat das neuere Profil, mit der höheren Profil-ID, die Priorität.

B - Standardprofile

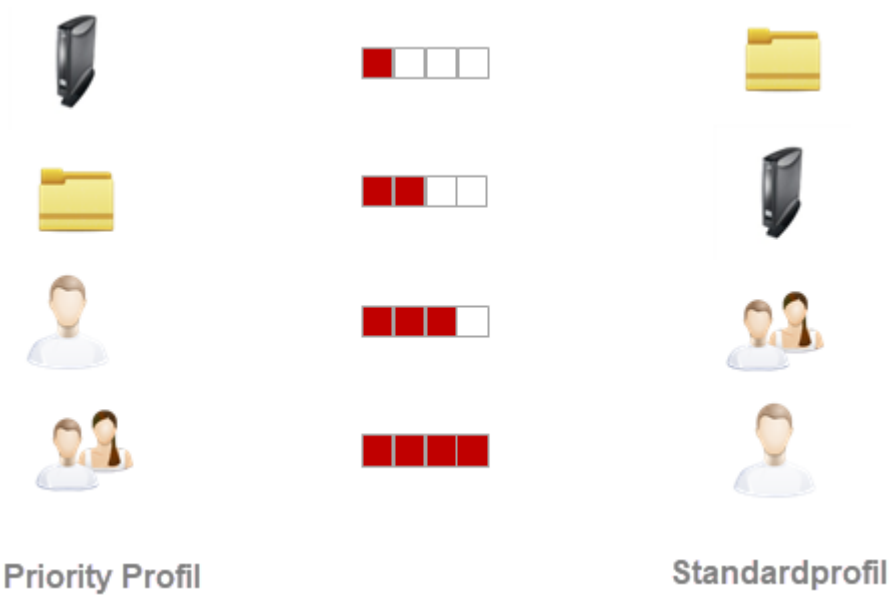
- Je näher das Standardprofil dem Gerät ist, umso höher ist seine Priorität.

C - Shared Workplace

- Je näher das Standardprofil dem Benutzer ist, umso höher ist seine Priorität.
- Profile, die Benutzern zugewiesen sind, haben höhere Priorität als Profile, die Geräten zugewiesen sind.
- Gruppen innerhalb einer Ebene werden in alphabetischer Reihenfolge priorisiert.

D - Priority Profile

- Priority Profile übersteuern alle Standardprofile.
- Einstellungen in Priority Profilen können nur von Priority Profilen überschrieben werden.
- Priority Profile sind hinsichtlich ihrer Priorisierung untereinander umgekehrt gestaffelt als die Standardprofile.
- Priority Profile, die näher am Objekt sind, haben weniger Priorität.
- Priority Profile, die Benutzergruppen zugewiesen sind, haben höhere Priorität als die, die einzelnen Benutzern zugewiesen sind. Diese haben höhere Priorität als Priority Profile, die Geräteverzeichnissen zugewiesen sind. Die niedrigste Priorität haben Priority Profile, die einem einzelnen Gerät zugewiesen sind.



Informationen zur Priorisierung von Firmwareanpassungen finden Sie unter Firmwareanpassungen in der IGEL UMS (see page 435).

Informationen zur Priorisierung von Universal Firmware Updates finden Sie unter Vorrang von IGEL UMS Profilen und Universal Firmware Updates (see page 201).

Priority Profile in der IGEL UMS

In der IGEL Universal Management Suite (UMS) können Sie Priority Profile (früher "Masterprofile" genannt) erstellen.

Ziel von Priority Profilen ist es, die Rechteverwaltung für UMS Administratoren in sehr großen oder verteilten Umgebungen abbilden zu können.

Mit Priority Profilen können höherrangige Administratoren Profileinstellungen von anderen Administratoren beeinflussen, ohne ihnen die Verwaltungsrechte für Standardprofile zu entziehen.

Menüpfad: **UMS Konsole > Priority Profile**

Wichtige Merkmale von Priority Profilen

- Priority Profile haben dieselbe Wirkungsweise wie Standardprofile, werden jedoch anders priorisiert. Nähere Informationen finden Sie unter Wirkungsordnung von Priority Profilen (see page 404).
- Priority Profile sind Profile, deren Einstellungen alle Standardprofile übersteuern.
- Priority Profile können von Standardprofilen nicht überschrieben werden.
- Priority Profile werden in einem eigenen Abschnitt im UMS Strukturbaum aufgeführt. Sie müssen jedoch erst aktiviert werden; siehe die Anleitung unten.

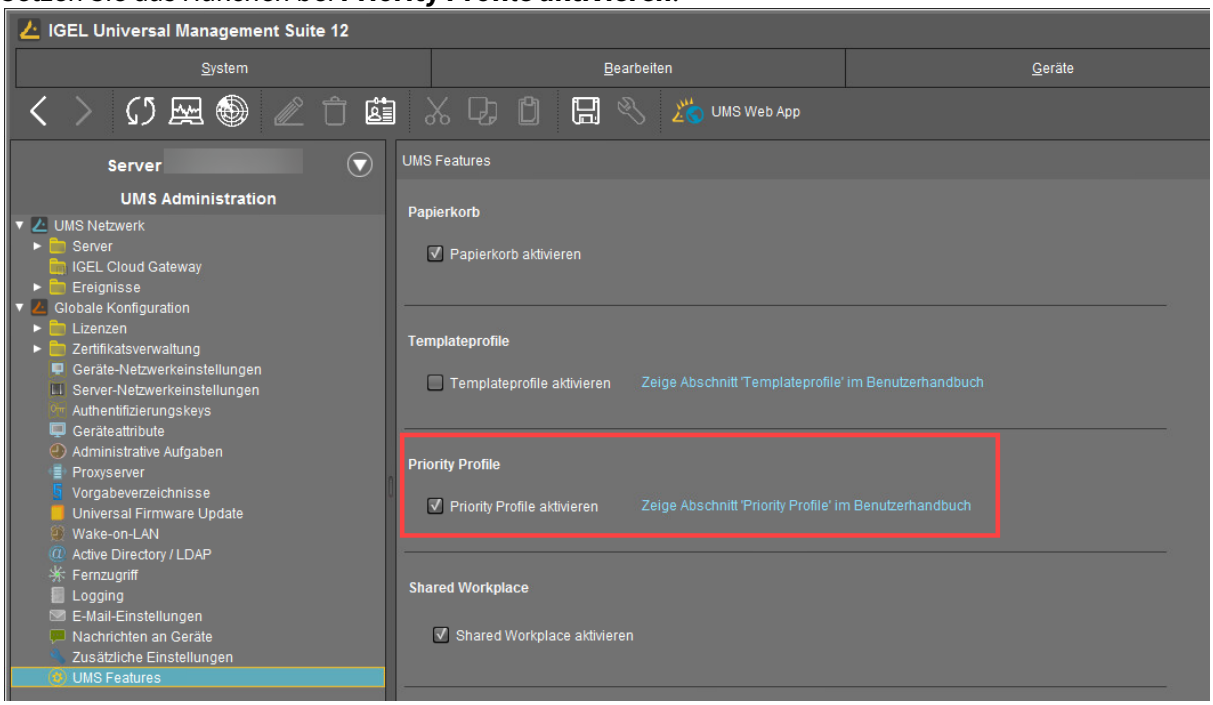
Priority Profile aktivieren

Standardmäßig ist die Funktion **Priority Profile** deaktiviert. Wenn Sie Priority Profile einsetzen möchten, gehen Sie wie folgt vor.

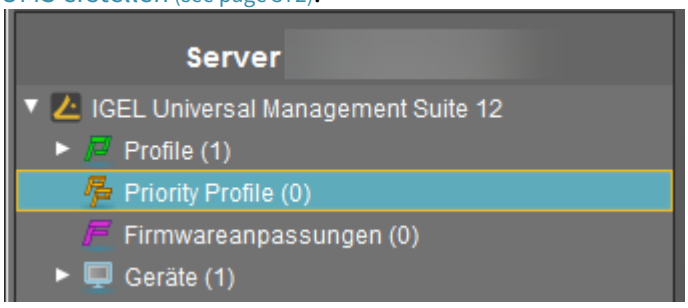
Über die UMS Konsole

1. Gehen Sie in der UMS Konsole zu **UMS Administration** > **Globale Konfiguration > UMS Features**.

2. Setzen Sie das Häkchen bei **Priority Profile aktivieren**.



Der Knoten **Priority Profile** erscheint im Strukturbaum. Sie können nun Priority Profile erstellen: Die Vorgehensweise ist identisch mit der Erstellung von Standardprofilen, siehe Profile in der IGEL UMS erstellen (see page 372).



Über die UMS Web App

1. Gehen Sie in der UMS Web App zum Bereich **Netzwerk > Einstellungen**.
2. Gehen Sie zum Tab **UMS-Funktionen**.
3. Setzen Sie das Häkchen bei **Priority Profile aktivieren**.

Weitere Informationen finden Sie unter Netzwerk-Einstellungen in der IGEL UMS Web App.

IGEL Tech Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=FZFPpdSe0lM

Templateprofile in der IGEL UMS

In der IGEL Universal Management Suite (UMS) können Sie Templateprofile verwenden. Templateprofile müssen erst unter **UMS Administration > Globale Konfiguration > UMS Features** aktiviert werden, siehe Templateprofile in der IGEL UMS aktivieren (see page 419).

Menüpfad: **UMS Konsole > Templateprofile**

Ein Templateprofil erlaubt es, einzelne Parameter im Profil mit Variablen zu belegen und deren Werte Objekten zuzuweisen.

> Sowohl **Standardprofile** als auch **Priority Profile** können durch den Einsatz von Variablen zu Templateprofilen werden.

Templateprofile werden eingesetzt, wenn man vermeiden möchte, viele Sitzungen anzulegen, die sich nur in wenigen Punkten unterscheiden.

> Templateprofile und Templateschlüssel können nicht verwendet werden, wenn Shared Workplace (see page 951) benutzt wird.

Anwendungsbeispiel

Die Geräte eines Unternehmens sind auf mehrere Niederlassungen verteilt. Alle Geräte sollen über ein Profil eine Browsersitzung mit gleichen Einstellungen erhalten, allerdings soll in den globalen Einstellungen für jede Niederlassung eine andere Startseite konfiguriert werden, außerdem soll der Sitzungsname für jede Niederlassung individuell gesetzt werden.

Bisherige Lösung

Bisher legt man für jede Niederlassung ein eigenes Profil mit globalen Einstellungen und Sitzungsdaten an.

Problem

Oft lassen sich die gewünschten Einstellungen über verschiedene Profile aber nicht kombinieren, siehe freie Instanzen (see page 369). Außerdem ist die unnötige Vielzahl an Profilen auf Dauer schwer zu verwalten.

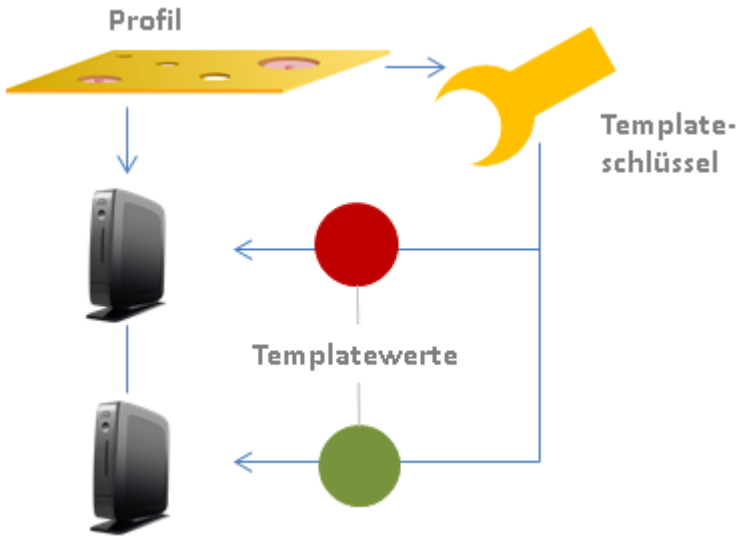
Lösung

Flexibler ist der Einsatz eines einzigen Templateprofils. Dieses enthält alle Daten für die Browsersitzung, die den Geräten gemeinsam sind und zusätzlich Platzhalter, sogenannte Templateschlüssel (see page 421). Die

Templateschlüssel enthalten Parameter, die für unterschiedliche Geräte an unterschiedlichen Standorten abweichende Werte erhalten sollen.

Das Templateprofil wird allen Geräten zugewiesen. Die standortbezogenen Templatewerte werden jeweils den Geräten zugewiesen, die diesen Templatewert erhalten sollen.

Das Gerät erhält damit ein Profil, dessen Einstellungen sich aus den fest im Profil gepflegten Parameterwerten und den ihm zugewiesenen Templatewerten zusammensetzt, die durch Templateschlüssel im Profil referenziert werden. Zusätzlich gibt es statische Templateschlüssel, die ihre Werte vom Gerät erhalten.



Regeln:

- Templateschlüssel werden in einem oder mehreren Profilen verwendet.
- Ein Templateschlüssel hat mehrere Werte.
- Das Templateprofil wird mehreren Geräten direkt oder indirekt zugewiesen.
- Ein Wert des Schlüssels kann jeweils einem oder mehreren Geräten direkt oder indirekt zugewiesen werden.

Ein Gerät erhält somit neben den allgemeinen Einstellungen des Profils auch den ihm zugewiesenen Templatewert für den Konfigurationsparameter, der im Profil durch den zugehörigen Templateschlüssel als Platzhalter repräsentiert ist.

IGEL Tech Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=uJnIK5u688c

- Templateprofile in der IGEL UMS aktivieren (see page 419)

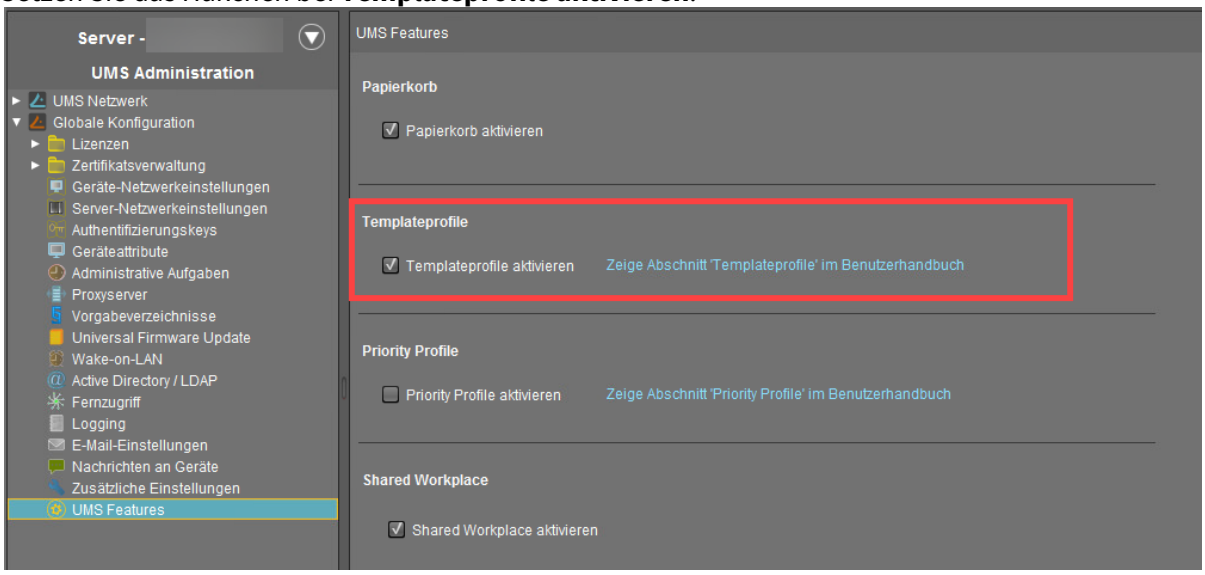
- Templateschlüssel und Werte erstellen (see page 421)
- Templateschlüssel in Profilen verwenden (see page 427)
- Templateprofile und Werte den Geräten zuordnen (see page 429)
- Wertesammlungen (see page 431)
- Templateschlüssel und Wertesammlungen exportieren (see page 433)
- Templateschlüssel und Wertesammlungen importieren (see page 434)

Templateprofile in der IGEL UMS aktivieren

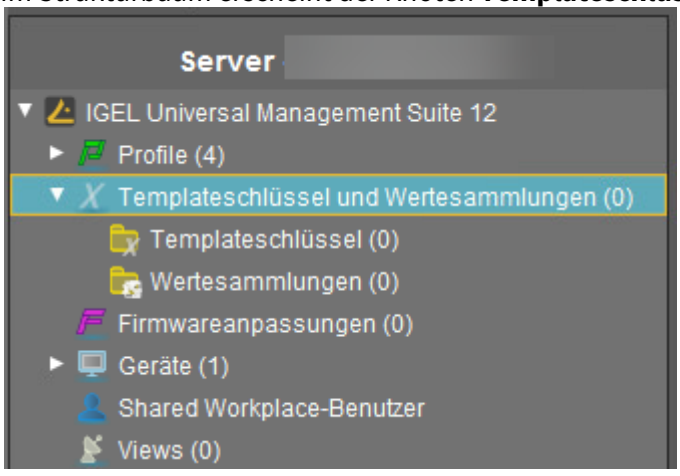
Wenn Sie die Funktion **Templateprofile** in der IGEL Universal Management Suite (UMS) nutzen möchten, müssen Sie diese erst über die UMS-Konsole oder die IGEL UMS Web App aktivieren.

Templateprofile in der UMS Console aktivieren

1. Gehen Sie in der UMS Konsole unter **UMS Administration > Globale Konfiguration > UMS Features**.
2. Setzen Sie das Häkchen bei **Templateprofile aktivieren**.



Im Strukturbaum erscheint der Knoten **Templateschlüssel und Wertesammlungen**.



Templateprofile in der UMS Web App aktivieren

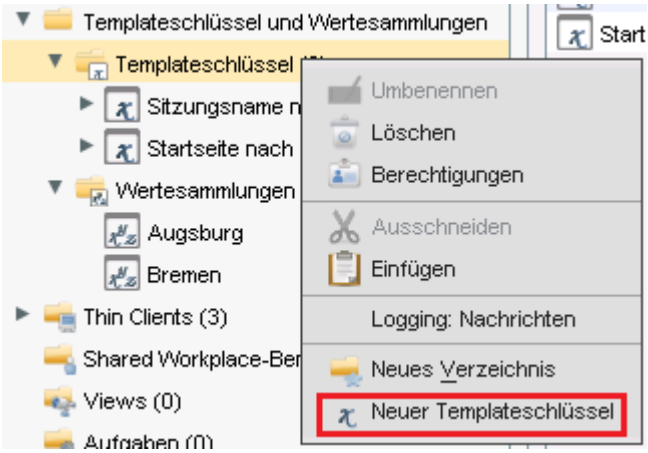
1. Gehen Sie in der UMS Web App zum Bereich **Netzwerk > Einstellungen**.
2. Gehen Sie zum Tab **UMS-Funktionen**.
3. Setzen Sie das Häkchen bei **Templateprofile aktivieren**.

Weitere Informationen finden Sie unter Netzwerk-Einstellungen in der IGEL UMS Web App (see page 897).

Templateschlüssel und Werte erstellen

So erstellen Sie Templateschlüssel und Werte:

1. Öffnen Sie das Kontextmenü des Verzeichnisses **Templateschlüssel**.
2. Klicken Sie **Neuer Templateschlüssel**.



> Alternativ ist diese Funktion auch erreichbar über das Menü **System > Neu > Neuer Templateschlüssel**, dazu muss der Fokus auf dem Knoten **Templateschlüssel** liegen.

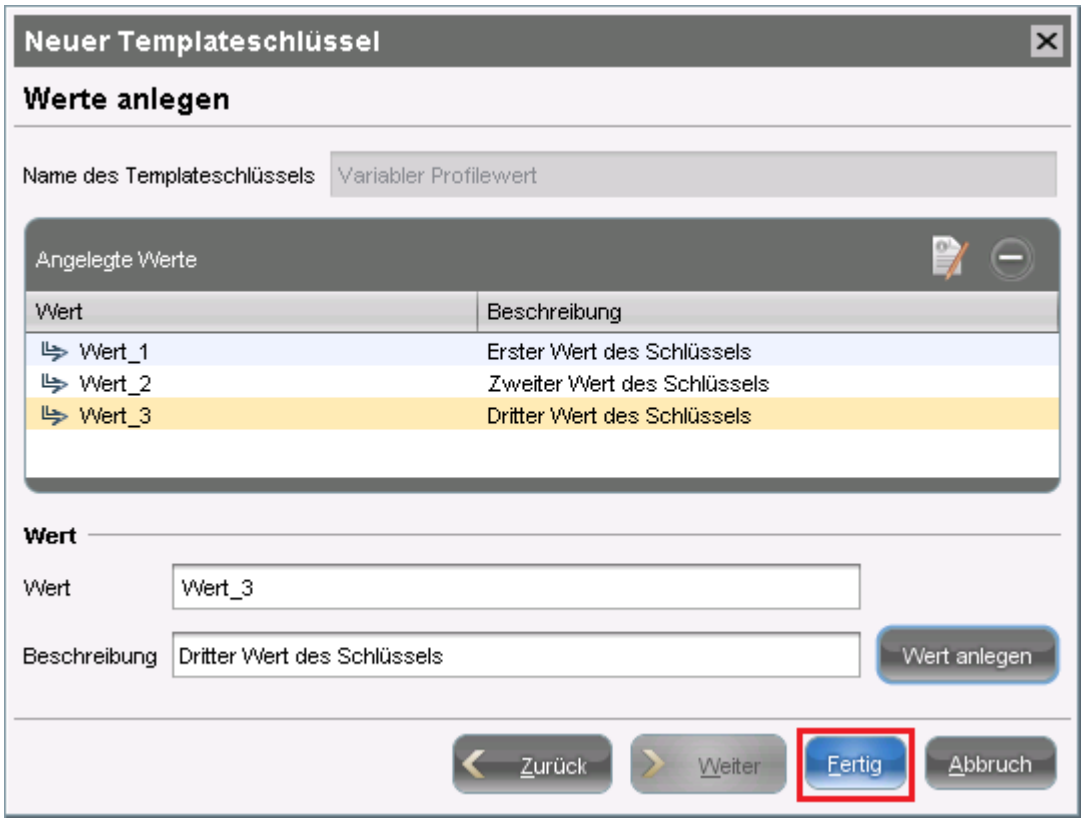
3. Definieren Sie einen **Namen** für den Schlüssel.
4. Wählen Sie einen **Werttyp** für den Schlüssel (Zeichenkette, Wahrheitswert, Ganz- oder Gleitkommazahl).
5. Erfassen Sie optional eine **Beschreibung** des Schlüssels.
6. Klicken Sie **Weiter**.

So legen Sie den ersten Wert des Schlüssels an:

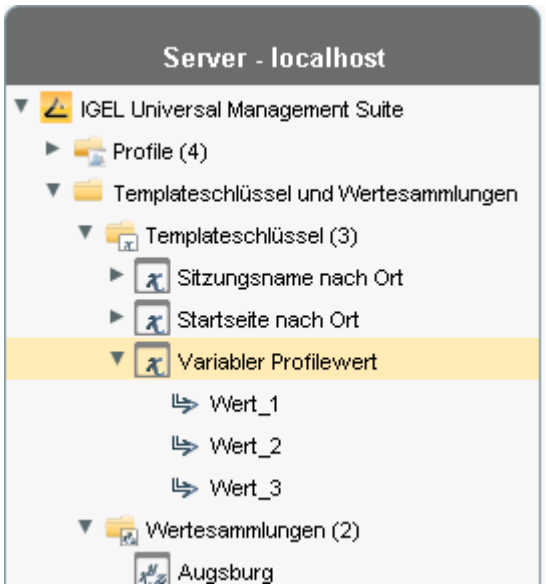
1. Erfassen Sie den gewünschten Parameterwert im Feld **Wert**.
2. Ergänzen Sie optional eine **Beschreibung** des Werts.
3. Klicken Sie **Wert anlegen**.

So legen Sie weitere Werte des Schlüssels an:

1. Ändern Sie die Eintragungen unter **Wert** und **Beschreibung**.
2. Klicken Sie **Wert anlegen**.
3. Klicken Sie **Fertig**, um den Schlüssel mit seinen Werten zu speichern, nachdem Sie alle gewünschten Werte angelegt haben.



Der Schlüssel wird mit seinen Werten im Baum angezeigt:



Als Workflow empfehlen wir, die Templateschlüssel und Werte aus der Profilkonfiguration (see page 425) heraus anzulegen.

Schlüssel und Werte im Profil erstellen

In Profilen lassen sich bestimmte Parameter mit Templateschlüssel konfigurieren. Damit verbinden Sie folgende Schritte zu einem Workflow:

- Templateschlüssel und Werte erstellen
- Templateschlüssel in Profilen verwenden

So nutzen Sie Templateschlüssel bei der Konfiguration eines Profils:

1. Öffnen Sie ein bestehendes Profil oder legen Sie ein neues Profil an.
2. Klicken Sie **Konfiguration bearbeiten**.
3. Wählen Sie einen Parameter, der einen clientspezifischen Wert aus einem Templateschlüssel beziehen soll.
4. Klicken Sie das Aktivierungssymbol vor dem Parameter, bis das Symbol  angezeigt wird.

   > Manche Parameter können nicht mit Templateschlüsseln konfiguriert werden und bieten nur die Optionen *inaktiv* und *aktiv*. Dies gilt z.B. für Kennwörter oder Parameter, die von anderen Konfigurationseinstellungen abhängig sind.

5. Klicken Sie das **Auswahlsymbol**  , um einen Templateschlüssel zu wählen.
6. Klicken Sie **Hinzufügen**  , um einen neuen Templateschlüssel anzulegen.
   Ein Assistent führt Sie durch die Schritte der Neuanlage:
7. Geben Sie einen **Namen** für den Schlüssel an.

   > Der **Werttyp** für den Schlüssel ist durch den Parameter vorgegeben.

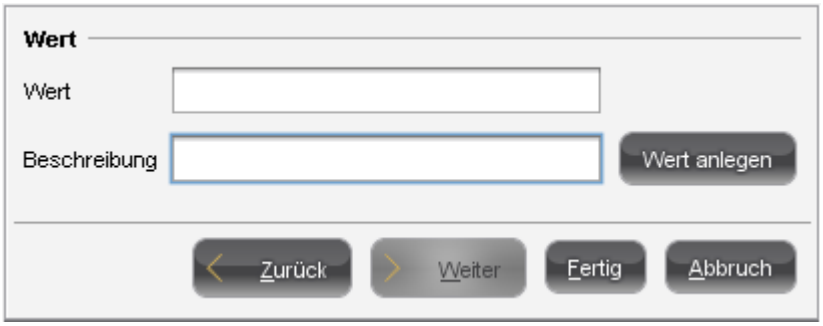
8. Geben Sie optional eine **Beschreibung** des Schlüssels an.

9. Klicken Sie **Weiter**.

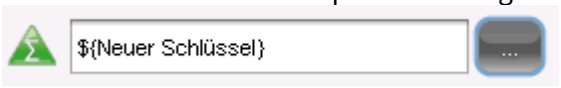
So erfassen Sie den ersten Wert des Schlüssels:

1. Definieren Sie den gewünschten Parameterwert im Feld **Wert**.
2. Ergänzen Sie optional eine **Beschreibung** des Werts.
3. Klicken Sie **Wert anlegen**.

> Bei Parametern mit festem Wertebereich, wie Auswahlmenü oder Checkbox, werden die vorhandenen Optionen zur Wahl gestellt. Klicken Sie **Alle anlegen**, um Werte für jeden Eintrag des Wertebereichs zu erstellen oder fügen Sie mit **Wert anlegen** nur ausgewählte Einträge hinzu.



4. Klicken Sie **Fertig**, um den Schlüssel mit seinen Werten zu speichern.
5. Klicken Sie **OK**, um in das Profil zurück zu gelangen.
   Der Schlüssel wird im Profilparameter angezeigt:



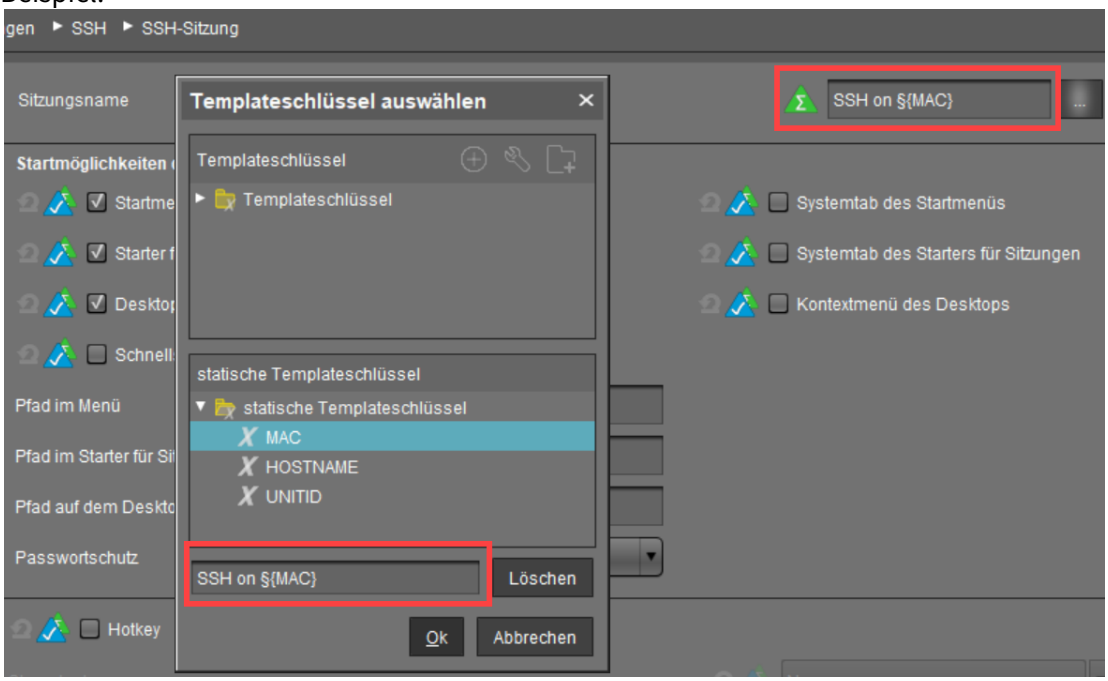
6. **Speichern** Sie das Templateprofil.
   Profile, die mindestens einen Templateschlüssel in der Konfiguration verwenden, werden im Navigationsbaum durch ein spezielles Symbol gekennzeichnet:  .

Templateschlüssel in Profilen verwenden

Templateschlüssel werden im Strukturbaum im Knoten **Templateschlüssel und Wertesammlungen / Templateschlüssel** aufgelistet. Sie lassen sich in eigene Unterverzeichnisse verschieben.

Statische Templateschlüssel sind im Strukturbaum nicht sichtbar; sie erhalten ihre Werte direkt vom Gerät. Statische Templateschlüssel sind mit dem Symbol § gekennzeichnet. Die folgenden statischen Templateschlüssel sind verfügbar:

- **MAC**: MAC-Adress des Geräts
- **HOSTNAME**: Hostname des Geräts
- **UNITID**: Unit ID des Geräts
  Beispiel:



So verwenden Sie einen Templateschlüssel im Profil:

1. Öffnen Sie ein bestehendes Profil oder legen Sie ein neues Profil an.
2. Rufen Sie in der Profilkonfiguration die zu pflegenden Parameter auf.
3. Wählen Sie einen Parameter, der mit clientspezifischen Werten aus einem Templateschlüssel versorgt werden soll.
4. Klicken Sie das Aktivierungssymbol vor dem Parameter, bis das Symbol  angezeigt wird.

	Der Parameter ist inaktiv und wird nicht durch das Profil konfiguriert.
	Der Parameter ist aktiv und der eingestellte Wert wird durch das Profil konfiguriert, Templateschlüssel sind für den Parameter nicht verfügbar.

	Der Parameter ist aktiv und der eingestellte Wert wird durch das Profil konfiguriert, Templateschlüssel sind für den Parameter verfügbar.
	Templateschlüssel sind aktiv für diesen Parameter, das Profil erhält hier später einen Wert des Schlüssels.
	Auf Standardwert zurücksetzen

> Diese und weitere Symbole sowie ihre Bedeutungen finden Sie unter **UMS Konsole > Hilfe > Legende**.

> Manche Parameter können nicht mit Templateschlüsseln konfiguriert werden und bieten nur die Optionen *inaktiv* und *aktiv*. Dies gilt z.B. für Kennwörter oder Parameter, die von anderen Konfigurationseinstellungen abhängig sind.

5. Klicken Sie das Auswahlsymbol  , um einen Templateschlüssel zu wählen.
6. Doppelklicken Sie den gewünschten **Templateschlüssel** oder legen Sie einen neuen Schlüssel an, siehe Schlüssel und Werte im Profil erstellen (see page 425).
7. Klicken Sie **OK**.
8. **Speichern** Sie das Templateprofil.
9. Sie können auch mehrere Templateschlüssel miteinander verketten:

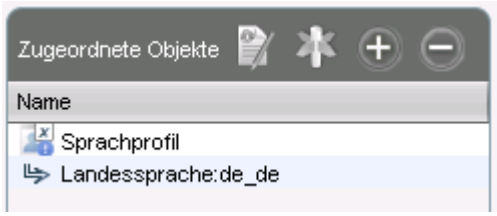
Profile, die mindestens einen Templateschlüssel in der Konfiguration verwenden, werden im Strukturbaum durch ein spezielles Symbol gekennzeichnet:  .

Templateprofile und Werte den Geräten zuordnen

Nachdem Sie die Templateschlüssel und Werte und die Konfiguration von Profilen unter Verwendung der Templateschlüssel angelegt haben, müssen Sie die Schlüssel und Werte am Gerät wieder zusammenführen.

So weisen Sie einem Gerät ein Templateprofil und die für die Ersetzung der Schlüssel notwendigen Werte zu:

1. Wählen Sie ein **Templateprofil** und ordnen Sie es wie üblich einer Gruppe von Geräten oder einem Geräteverzeichnis zu.
2. Wählen Sie zu jedem im Profil verwendeten Templateschlüssel einen Wert aus.
3. Ordnen Sie die jeweiligen Werte den entsprechenden Geräts über die Liste **Zugeordnete Objekte** zu.



4. Ordnen Sie weitere Werte der Schlüssel weiteren Geräte zu. Es lassen sich auch mehrere Werte verschiedener Schlüssel gesammelt zuordnen (Tasten [Umschalt]und [Strg]).

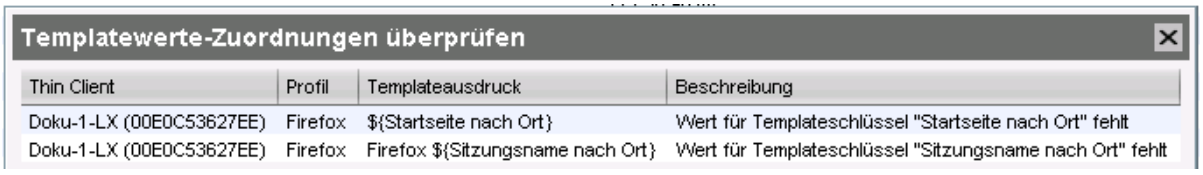
> ⓘ Jedes Gerät muss anschließend für jeden Schlüssel in den zugewiesenen Profilen auch einen zugewiesenen Wert besitzen.

So prüfen Sie, ob die Zuordnung von Templateprofilen und Templatewerten vollständig ist:

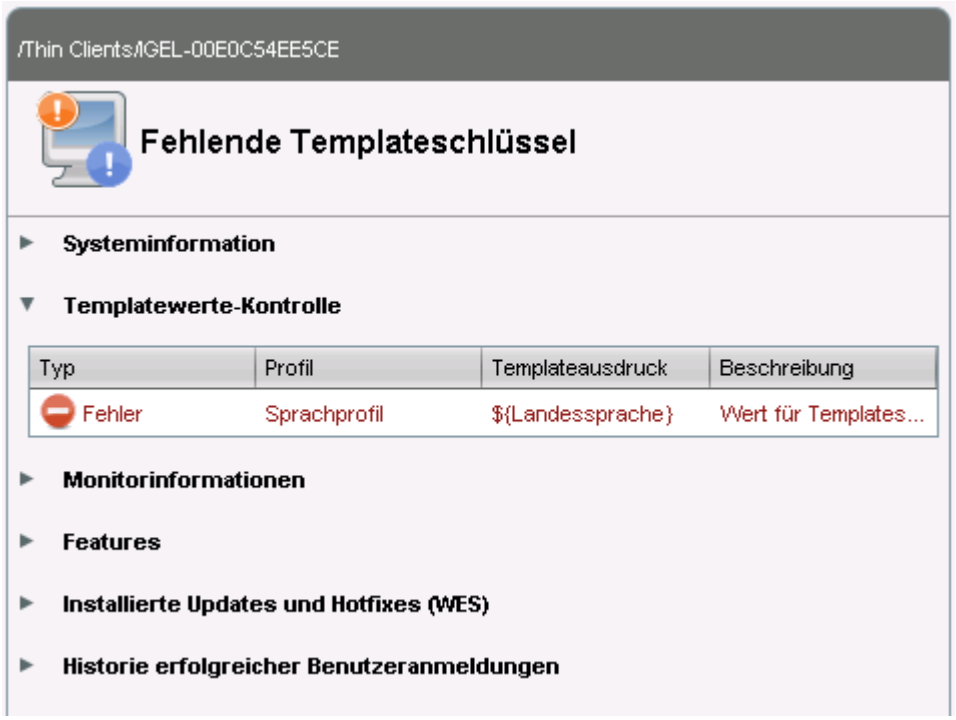
1. Klicken Sie in der oberen Menüleiste **Geräte**.
2. Wählen sie **Templatewerte-Zuordnungen überprüfen**.
   Die ausgewählten und geprüften Geräte werden dem Ergebnis entsprechend gekennzeichnet:

	alle Templateschlüssel sind definiert
	fehlende Templateschlüssel

3. Doppelklicken Sie auf die Meldung im Nachrichtenfenster, um das Fehlerprotokoll der Prüfung zu öffnen:



   Alternativ klicken Sie ein Gerät, auch hier werden die Prüfergebnisse direkt angezeigt:



Sobald die Geräte ihre aktualisierten Profileinstellungen erhalten (z. B. automatisch nach dem Neustart der Geräte), werden für jedes Gerät die im Profil enthaltenen Schlüssel durch den entsprechenden Wert aus deren Zuordnung zum Gerät ersetzt und an das Gerät übermittelt. Das lokale Setup des Geräts enthält somit nur die üblichen Parameterwerte und keine Schlüssel mehr.

Wertesammlungen

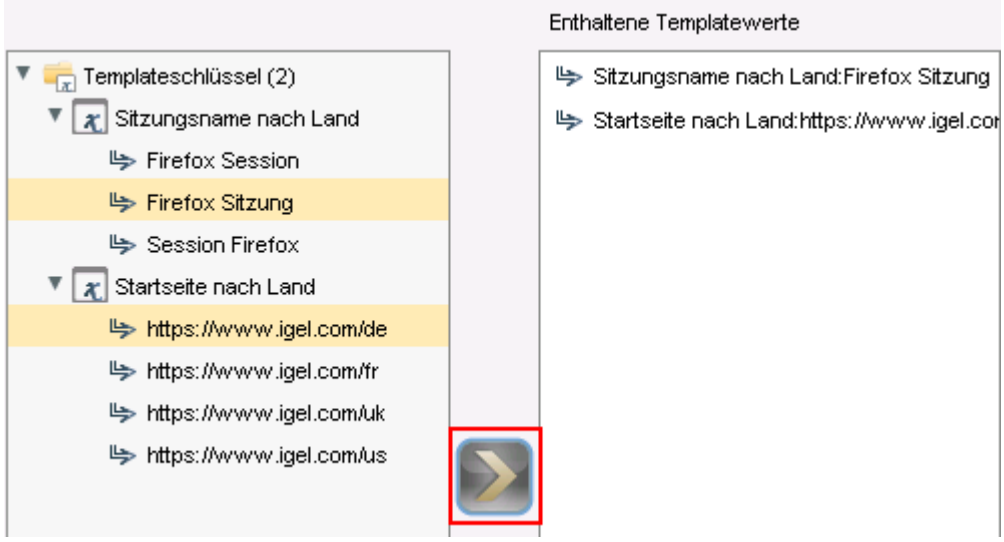
In Wertesammlungen lassen sich logisch zusammengehörige Werte verschiedener Templateschlüssel zusammenfassen und gemeinsam Geräten zuordnen.

Haben Sie z.B. verschiedene Profile, die länderspezifische Einstellungen über Templateschlüssel und Wertzuweisungen erhalten sollen, so können alle Werte für ein Land / eine Sprache in einer Wertesammlung gruppiert werden. Ein Gerät erhält mit Zuordnung einer solchen Sammlung auch alle darin enthaltenen Werte für sein Land / seine Sprache.

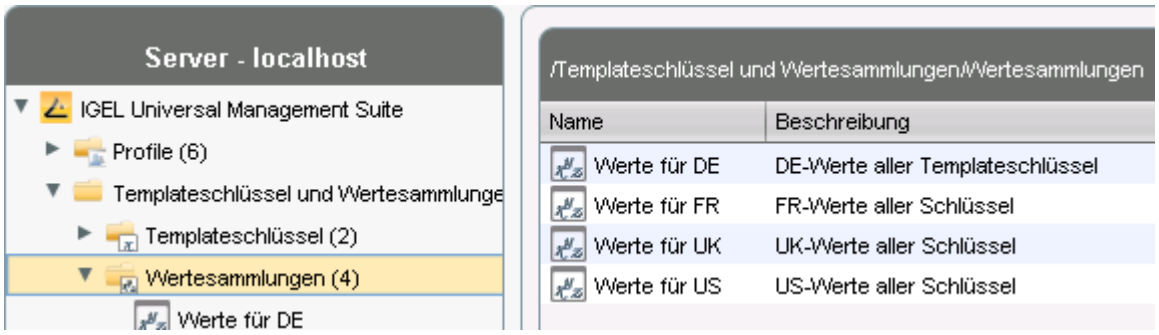
So legen Sie eine Wertesammlung an:

1. Legen Sie ein Templateprofil mit Schlüsseln und Werten an.
2. Klicken Sie **System > Neu > Neue Wertesammlung**, um eine neue Wertesammlung anzulegen.
3. Tragen Sie **Namen** und **Beschreibung** für die Sammlung ein.

4. Wählen Sie aus jedem Schlüssel die gewünschten Werte aus, eine Mehrfachauswahl ist möglich.



5. Bestätigen Sie mit **OK**.
6. Legen sie weitere Wertesammlungen an.



7. Weisen Sie das Templateprofil allen Geräte zu.
8. Weisen Sie den Geräten jeweils die passende Wertesammlung zu.
9. Markieren Sie den Baumknoten **Geräte**.
10. Klicken Sie im Menü unter **Geräte > Templatewerte-Zuordnungen prüfen**, um die Zuordnungen zu prüfen.
    Das Ergebnis wird Ihnen im Nachrichtenfenster angezeigt.

Die Geräte erhalten beim nächsten Neustart oder nach manueller Übermittlung die neuen Sitzungsdaten mit gemeinsamen und länderspezifischen Einstellungen des Profils.

> Der Vorteil dieser Methode ist, dass Sie in Zukunft weitere Schlüsselwerte nur noch der entsprechenden Wertesammlung hinzufügen müssen, um diese den Geräten der Niederlassung zuzuweisen. Zusätzlich verbessert sich die Übersicht bei großer Zahl an Templateschlüsseln und Werten.

Templateschlüssel und Wertesammlungen exportieren

Menüpfad: **System > Exportieren > Templateschlüssel und Wertesammlungen exportieren**

Sie können die in der UMS Datenbank vorhandenen Templateschlüssel und Wertesammlungen exportieren, um sie in eine andere UMS Installation zu importieren.

So exportieren Sie Templateschlüssel und Wertesammlungen:

1. Wenn Sie eine Vorauswahl treffen wollen, markieren Sie im Navigationsbaum die gewünschten Templateschlüssel und Wertesammlungen oder Verzeichnisse.
2. Gehen Sie zu **System** > **Exportieren** > **Templateschlüssel und Wertesammlungen exportieren**.
   Im Fenster **Templateschlüssel und Wertesammlungen exportieren** werden die zuvor ausgewählten Templateschlüssel und Wertesammlungen oder alle verfügbaren Templateschlüssel und Wertesammlungen angezeigt.
3. Wählen Sie in der Spalte **Exportieren** die Templateschlüssel und Wertesammlungen, die Sie exportieren wollen.
4. Klicken Sie **Weiter** und wählen Sie einen Speicherort aus.
5. Klicken Sie **Fertig**.
   Die Templateschlüssel und Wertesammlungen werden in einem ZIP-Archiv gespeichert.

Templateschlüssel und Wertesammlungen importieren

Menüpfad: **System > Exportieren > Templateschlüssel und Wertesammlungen importieren**

Sie können Templateschlüssel und Wertesammlungen importieren. Bedingung hierfür ist, dass die zu importierenden Templateschlüssel noch nicht in der UMS Datenbank existieren. Jeder Templateschlüssel hat einen eindeutigen Namen, der nur einmal in einer UMS Datenbank vorkommen darf.

So importieren Sie Templateschlüssel und Wertesammlungen:

1. Markieren Sie im Navigationsbaum das Verzeichnis, in dem die Templateschlüssel und Wertesammlungen abgelegt werden sollen.

   > Wenn Sie Templateschlüssel und Wertesammlungen in einem einzigen Vorgang importieren wollen, beachten Sie Folgendes: Wenn ein Verzeichnis unterhalb von **Templateschlüssel** ausgewählt ist, werden die Templateschlüssel im ausgewählten Verzeichnis abgelegt, und die Wertesammlungen im Verzeichnis **Wertesammlungen**. Wenn ein Verzeichnis unterhalb von **Wertesammlungen** ausgewählt ist, werden die Wertesammlungen im ausgewählten Verzeichnis abgelegt, und die Templateschlüssel im Verzeichnis **Templateschlüssel**.

2. Gehen Sie zu **System** > **Importieren** > **Templateschlüssel und Wertesammlungen importieren**.
3. Wählen Sie die Datei mit den Templateschlüssel und Wertesammlungen und klicken Sie **Öffnen**.
   Das Fenster **Templateschlüssel und Wertesammlungen** öffnet sich.
4. Wählen Sie in der Spalte **Importieren** die zu importierenden Templateschlüssel und Wertesammlungen aus.
5. Legen Sie mit der Option **Erzeuge Pfad relativ zum derzeit selektierten Verzeichnis** fest, ob die Verzeichnisstruktur der importierten Templateschlüssel und Wertesammlungen erhalten bleiben soll:
   ☑ Die Verzeichnissstruktur der importierten Templateschlüssel und Wertesammlungen bleibt erhalten, d. h. die exportierten Unterverzeichnisse werden wiederhergestellt. (Standard)
   ☐ Die Verzeichnissstruktur der importierten Templateschlüssel und Wertesammlungen wird ignoriert, d. h. alle Templateschlüssel und Wertesammlungen werden auf der obersten Verzeichnisebene abgelegt.
6. Klicken Sie **Ok**.
   Wenn alle Templateschlüssel und Wertesammlungen importiert wurden, wird eine Bestätigung angezeigt.
   Wenn nicht alle Templateschlüssel und Wertesammlungen importiert werden konnten, werden die Templateschlüssel und Wertesammlungen angezeigt, bei denen der Import fehlschlug.

Firmwareanpassungen in der IGEL UMS

Mithilfe der Firmwareanpassungsfunktion in der IGEL Universal Management Suite (UMS) können Sie die Benutzeroberfläche Ihrer IGEL OS Geräte an Ihr Corporate Design anpassen. Die Konfiguration erfolgt in einem eigenen Wizard; für eine Minimalkonfiguration genügt es, einen Namen und ein Dateiobjekt anzugeben.

Menüpfad: **UMS Konsole > Firmwareanpassungen**

Wirkungsweise

Eine Firmwareanpassung kann sowohl einem Gerät als auch einem Verzeichnis zugewiesen werden.

Firmwareanpassungen übersteuern Standardprofile, können aber ihrerseits von Priority Profilen übersteuert werden. Sie liegen also in der Priorisierung zwischen Priority Profilen und Standardprofilen. Weitere Informationen zur Priorisierung von Profilen finden Sie unter Priorisierung von Profilen in der IGEL UMS (see page 398).

Wenn einem Gerät mehrere Anwendungsfälle desselben Typs zugewiesen werden, z. B. ein Hintergrundbild, wird nur der Anwendungsfall mit der höchsten Priorität wirksam. Die Priorität ergibt sich daraus, wie direkt oder indirekt die Zuweisung zum Gerät ist: Eine direkt dem Gerät zugewiesene Firmwareanpassung hat eine höhere Priorität als eine Firmwareanpassung, die dem Geräteverzeichnis zugewiesen ist. Wenn beide Firmwareanpassungen die gleiche Priorität haben, ist die Firmwareanpassung mit der höheren ID wirksam.

> Um die ID einer Firmwareanpassung zu erhalten, fahren Sie im Strukturbaum mit dem Mauszeiger über das betreffende Objekt.

- Firmwareanpassung erstellen (see page 436)
- Firmwareanpassungen exportieren (see page 445)
- Firmwareanpassungen importieren (see page 446)

Firmwareanpassung erstellen

So erstellen Sie eine **Firmwareanpassung**:

1. Setzen Sie den Cursor im Strukturbaum auf **Firmwareanpassung**.
2. Wählen Sie im Kontextmenü **Neue Firmwareanpassung erstellen**.
   Das Dialogfenster **Firmwareanpassung Details** wird angezeigt.
3. Vergeben Sie einen **Namen** für diese Firmwareanpassung.
4. Wählen Sie einen **Anwendungsfall** aus. Wählbar sind:
   - Startmenüsymbol (see page 437)
   - Startmenü (see page 438)
   - Hintergrund der Taskleiste (see page 439)
   - Bildschirmschoner (see page 440)
   - Bildschirmschoner (Custom Partition) (see page 441)
   - Bootsplash (see page 443)
   - Hintergrundbild (see page 444)
5. Klicken Sie **Weiter**.
   Das Dialogfenster **Firmwareanpassung Zuweisung** wird angezeigt.
6. Markieren Sie ein oder mehrere Verzeichnisse oder Geräte und klicken Sie , um die Firmwareanpassung zuzuweisen.
7. Klicken Sie **Fertig**.

Die angelegten Firmwareanpassungen werden im Strukturbaum unterhalb des Knotens **Firmwareanpassungen** aufgelistet. Wenn Sie eine Firmwareanpassung anklicken, werden Ihnen die zugehörigen Dateien und die zugeordneten Objekte angezeigt.

Die in einer Firmwareanpassung verwendeten Dateien werden mit einem gekennzeichnet.

> Wenn Sie eine mit gekennzeichnete Datei löschen wollen, müssen Sie diese zuerst aus der dazugehörigen Firmwareanpassung entfernen.

Die Einstellungen eines Anwendungsfalls können für eine Firmwareanpassung aktiviert oder deaktiviert werden, wie Sie es schon von den Profilen kennen:

	Der Parameter ist inaktiv und wird nicht durch die Firmwareanpassung konfiguriert.
	Der Parameter ist aktiv und der eingestellte Wert wird durch die Firmwareanpassung konfiguriert.

> Ausnahme: Der Dateipfad bei Bildschirmschoner (Custom partition) kann nicht deaktiviert werden.

Startmenüsymbol

Firmwareanpassung Details

- **Name**: Name der Firmwareanpassung
- **Anwendungsfall**: "Startmenü-Symbol"
- **Bild**: Name der ausgewählten Bilddatei
- **Datei auswählen**: Hier werden alle in der UMS registrierten Dateien angezeigt, die im geeigneten Format (*.png, *ico) vorliegen und für die Sie Berechtigungen haben.
- **Datei hochladen**: Wählen Sie eine Datei aus einem lokalen Verzeichnis oder aus dem UMS Server aus.
- **Löschen**: Entfernt die unter **Bild** angezeigte Bilddatei.

Firmwareanpassung Zuweisung

Zuordnung der Geräte, für die die Anpassungen gelten sollen.

Startmenü

Firmwareanpassung Details

- **Name**: Name der Firmwareanpassung
- **Anwendungsfall**: "Startmenü"
- **Bild**: Name der ausgewählten Bilddatei
- **Datei auswählen**: Hier werden alle in der UMS registrierten Dateien angezeigt, die im geeigneten Format (*.jpg, *bmp, *png) vorliegen und für die Sie Berechtigungen haben.
- **Datei hochladen**: Wählen Sie eine Datei aus einem lokalen Verzeichnis oder aus dem UMS Server aus.
- **Löschen**: Entfernt die unter **Bild** angezeigte Bilddatei.

Firmwareanpassung Zuweisung

Zuordnung der Geräte, für die die Anpassungen gelten sollen.

Hintergrund der Taskleiste

Firmwareanpassung Details

- **Name**: Name der Firmwareanpassung
- **Anwendungsfall**: "Hintergrund der Taskleiste"
- **Bild**: Name der ausgewählten Bilddatei
- **Datei auswählen**: Hier werden alle in der UMS registrierten Dateien angezeigt, die im geeigneten Format (*.jpg, *bmp, *png) vorliegen und für die Sie Berechtigungen haben.
- **Datei hochladen**: Wählen Sie eine Datei aus einem lokalen Verzeichnis oder aus dem UMS Server aus.
- **Löschen**: Entfernt die unter **Bild** angezeigte Bilddatei.

Firmwareanpassung Zuweisung

Zuordnung der Geräte, für die die Anpassungen gelten sollen.

Bildschirmschoner

Firmwareanpassung Details

- **Name**: Name der Firmwareanpassung
- **Anwendungsfall**: "Bildschirmschoner"
- **Bilder**: Namen der ausgewählten Bilddateien
- **Datei auswählen**: Hier werden alle in der UMS registrierten Dateien angezeigt, die im geeigneten Format (*.jpg, *bmp, *png) vorliegen und für die Sie Berechtigungen haben.
- **Datei hochladen**: Wählen Sie eine Datei aus einem lokalen Verzeichnis oder aus dem UMS Server aus.
- **Löschen**: Entfernt die unter **Bild** angezeigte Bilddatei.
- **Anzeigemodus**: Art der Anzeige.
  Mögliche Optionen:
  - nebeneinander klein
  - nebeneinander mittelgroß
  - mittig zentriert
  - beschneiden
- **Bildmodus**:
  - Ein Bild pro Monitor
  - Ein Bild für alle Monitore (gestreckt falls nötig)
- **Anzeigedauer pro Bild**: Zeit in Sekunden an, die ein Bild angezeigt werden soll, bevor es wechselt. (Standard: 10)
- **Start**
  Mögliche Optionen:
  - Bildschirmschoner automatisch starten
  - Bildschirmschoner nicht automatisch starten
- **Startzeit**: Zeit in Minuten, bis der Bildschirmschoner startet. (Standard: 5)
- **Hintergrundfarbe**: (Standard: schwarz)
  - **Wähle Farbe**: Farbauswahl nach Farbräumen
    Mögliche Farbräume:
    Swatches
    HSV
    HSL
    RGB
    CMYK

Firmwareanpassung Zuweisung

Zuordnung der Geräte, für die die Anpassungen gelten sollen.

Bildschirmschoner (Custom Partition)

Firmwareanpassung Details

- **Name**: Name der Firmwareanpassung
- **Anwendungsfall**: "Bildschirmschoner (Custom Partition)"
- **Bilder**: Namen der ausgewählten Bilddateien
- **Datei auswählen**: Hier werden alle in der UMS registrierten Dateien angezeigt, die im geeigneten Format (*.jpg, *bmp, *png) vorliegen und für die Sie Berechtigungen haben. Sie können hier mehrere Bilder auswählen.
- **Datei hochladen**: Wählen Sie eine Datei aus einem lokalen Verzeichnis oder aus dem UMS Server aus.
- **Löschen**: Entfernt die ausgewählten Bilddateien.

Dateipfad (Custom Partition + Ordner): Dateipfad eines Ordners auf der Custom Partition (Beispiel: `/custom/screensaver`).

> Die Custom Partition muss vorher angelegt sein, damit sie mit den Bildern bestückt werden kann. Wenn keine Custom Partition angelegt ist, werden die Bilder im RAM gespeichert und bei jedem Booten neu geladen. Der Ordner muss nicht im Voraus angelegt sein, er wird ggf. erstellt. Stellen Sie sicher, dass der Pfad mit einem `/` beginnt.

- **Anzeigemodus**: Art der Anzeige. Wählbar sind:
  - Klein, springend
  - Mittelgroß, springend
  - Ausgefüllt
  - Eingepasst
- **Bildmodus**:
  - Ein Bild pro Monitor
  - Ein Bild für alle Monitore (gestreckt falls nötig)
- **Anzeigedauer pro Bild**: Zeit in Sekunden, die ein Bild angezeigt werden soll, bevor es wechselt. (Standard: 10)
- **Start**
  Mögliche Optionen:
  - Bildschirmschoner automatisch starten
  - Bildschirmschoner nicht automatisch starten
- **Startzeit**: Zeit in Minuten, bis der Bildschirmschoner startet. (Standard: 5)
- **Hintergrundfarbe**: (Standard: schwarz)
  - **Wähle Farbe**: Farbauswahl nach Farbräumen
    Mögliche Farbräume:
    Swatches
    HSV
    HSL
    RGB
    CMYK

Firmwareanpassung Zuweisung

Zuordnung der Geräte, für die die Anpassungen gelten sollen.

Bootsplash

Firmwareanpassung Details

- **Name**: Name der Firmwareanpassung
- **Anwendungsfall**: "Bootsplash"
- **Bild**: Name der ausgewählten Bilddatei
- **Datei auswählen**: Hier werden alle in der UMS registrierten Dateien angezeigt, die im geeigneten Format (*.jpg, *bmp, *png) vorliegen und für die Sie Berechtigungen haben.
- **Datei hochladen**: Wählen Sie eine Datei aus einem lokalen Verzeichnis oder aus dem UMS Server aus.

  > Für den Bootsplash bezieht das Gerät die ausgewählte Datei von der UMS über HTTPS, sobald sie benötigt wird.

- **Löschen**: Entfernt die unter **Bild** angezeigte Bilddatei.
- **Horizontale Position**: Position des Bootsplash in der waagerechten. (Standard: 50%)
- **Vertikale Position**: Position des Bootsplash in der senkrechten. (Standard: 50%)
- **Fortschrittsanzeige (horizontal)**: Position der Fortschrittsanzeige in der waagerechten. (Standard: 90%)
- **Forschrittsanzeige (vertikal)**: Position der Fortschrittsanzeige in der senkrechten. (Standard: 90%)

Firmwareanpassung Zuweisung

Zuordnung der Geräte, für die die Anpassungen gelten sollen.

Hintergrundbild

Firmwareanpassung Details

- **Name**: "Hintergrundbild"
- **Anwendungsfall**: "Hintergrundbild"
- **Hintergrund Monitor 1-8**: Name jeweils einer Bilddatei für bis zu 8 Monitore
- **Datei auswählen**: Hier werden alle in der UMS registrierten Dateien angezeigt, die im geeigneten Format (*.jpg, *bmp, *png) vorliegen und für die Sie Berechtigungen haben.
- **Datei hochladen**: Wählen Sie eine Datei aus einem lokalen Verzeichnis oder aus dem UMS Server aus.

  > Für das Hintergrundbild bezieht das Gerät die ausgewählte Datei von der UMS über HTTPS, sobald sie benötigt wird.

- **Löschen**: Entfernt die unter **Hintergrund Monitor 1-8** angezeigte Bilddatei.

Firmwareanpassung Zuweisung

Zuordnung der Geräte, für die die Anpassungen gelten sollen.

Firmwareanpassungen exportieren

Menüpfad: **System > Exportieren > Firmwareanpassungen exportieren**

Sie können Firmwareanpassungen exportieren. Die exportierten Daten enthalten alle benötigten Einstellungen und Dateien.

So exportieren Sie Firmwareanpassungen:

1. Wenn Sie eine Vorauswahl treffen wollen, markieren Sie im Navigationsbaum die gewünschten Firmwareanpassungen oder Verzeichnisse.
2. Gehen Sie zu **System** > **Exportieren** > **Firmwareanpassungen exportieren**.
   Im Fenster **Firmwareanpassungen exportieren** werden die zuvor ausgewählten Firmwareanpassungen oder alle verfügbaren Firmwareanpassungen angezeigt.
3. Wählen Sie in der Spalte **Exportieren** die Firmwareanpassungen, die Sie exportieren wollen.
4. Klicken Sie **Weiter** und wählen Sie einen Speicherort aus.
5. Klicken Sie **Fertig**.
   Die Firmwaredaten werden in einem ZIP-Archiv gespeichert.

Firmwareanpassungen importieren

Menüpfad: **System > Importieren > Firmwareanpassungen importieren**

Sie können Firmwareanpassungen importieren. Die importierten Daten enthalten neben den Einstellungen alle benötigten Dateien.

So importieren Sie Firmwareanpassungen:

1. Markieren Sie das Verzeichnis, in dem die Firmwareanpassungen abgelegt werden sollen.
2. Gehen Sie zu **System** > **Importieren** > **Firmwareanpassungen importieren**.
3. Wählen Sie die Datei mit den Firmwareanpassungen und klicken Sie **Öffnen**.
   Das Fenster **Importiere Firmwareanpassungen** öffnet sich.
4. Wählen Sie in der Spalte **Importieren** die zu importierenden Firmwareanpassungen aus.
5. Legen Sie mit der Option **Erzeuge Pfad relativ zum derzeit selektierten Verzeichnis** fest, ob die Verzeichnissstruktur der importierten Firmwareanpassungen erhalten bleiben soll:
   ☑ Die Verzeichnissstruktur der importierten Firmwareanpassungen bleibt erhalten, d. h. die exportierten Unterverzeichnisse werden wiederhergestellt. (Standard)
   ☐ Die Verzeichnissstruktur der importierten Firmwareanpassungen wird ignoriert, d. h. alle Firmwareanpassungen werden auf der obersten Verzeichnisebene abgelegt.
6. Klicken Sie **Ok**.
   Wenn alle Firmwareanpassungen importiert wurden, wird eine Bestätigung angezeigt.
   Wenn nicht alle Firmwareanpassungen importiert werden konnten, werden die Firmwareanpassungen angezeigt, bei denen der Import fehlschlug.

Geräte

Menüpfad: Strukturbaum **> Geräte**

Im Bereich **Geräte** können Sie die am UMS Server registrierten Endgeräte verwalten. Alle am UMS Server registrierten Geräte werden angezeigt.

Der im Strukturbaum angezeigte Name eines Geräts dient zur Kennzeichnung in der UMS und muss nicht mit dem Namen des Geräts im Netzwerk identisch sein. Der im Strukturbaum angezeigte Name muss nicht eindeutig sein und kann mehrfach verwendet werden.

Die Unit ID dient als eindeutiges Identifizierungsmerkmal. Bei IGEL Geräten, IGEL Zero Clients, Geräten, die mit IGEL UDC/OSC konvertiert wurden, sowie Geräten mit IGEL UMA wird die Unit ID mit der MAC-Adresse des Geräts belegt.

Sie können den Bereich **Geräte** strukturieren, indem Sie Verzeichnisse und gegebenenfalls Unterverzeichnisse anlegen. Dabei ist zu beachten, dass jedes Gerät im Strukturbaum nur einmal angezeigt werden kann. Sie können ein Gerät per Drag & Drop von einem Verzeichnis in ein anderes verschieben.

Symbole für IGEL OS Geräte

Die folgenden Symbole im Strukturbaum zeigen den Status eines IGEL OS Geräts an:

> Wenn das Gerät über den IGEL Cloud Gateway (ICG) verbunden ist, erhält das Gerät ein Wolkensymbol  .

	Das Gerät ist online. Bitte beachten Sie, dass **Einstellungen > Onlineprüfung > Prüfe, ob die Geräte online sind** aktiviert sein muss, um den Online-Status anzuzeigen.
	Das Gerät ist offline. Bitte beachten Sie, dass **Einstellungen > Onlineprüfung > Prüfe, ob die Geräte online sind** aktiviert sein muss, um den Online-Status anzuzeigen.
	Änderungen wurden noch nicht zum Gerät übertragen (ist bei allen Status möglich).

Um die nachfolgenden Statusanzeigen zu aktivieren, muss die Option **Geräte senden Status-Updates** unter **UMS Administration > Globale Konfiguration > Geräte-Netzwerkeinstellungen > Updates für erweiterten Gerätestatus** aktiviert sein (Standard)

	Das Gerät zeigt den Anmeldebildschirm (falls konfiguriert).
	Das Gerät wird gerade aktualisiert.
	Die UMS hat keine Lizenz für das Gerät.
	Das Gerät war noch nie gemeldet.

Die UMS überwacht den Status der Geräte durch regelmäßiges Senden von UDP-Paketen. Gemäß Voreinstellung geschieht dies alle 3 Sekunden. Sie können das Abfrageintervall für die Onlineprüfung im Menü **Extras > Einstellungen > Onlineprüfung** festlegen. Zusätzlich können Sie den Status manuell aktualisieren.

Symbole für UD Pockets

Die folgenden Symbole im Strukturbaum zeigen den Status eines UD Pocket an:

	Registrierter UD Pocket (keine weiteren Informationen).
	Der UD Pocket ist online. Das Gerät ist offline. Bitte beachten Sie, dass **Einstellungen > Onlineprüfung > Prüfe, ob die Geräte online sind** aktiviert sein muss, um den Online-Status anzuzeigen.
	Der UD Pocket ist offline. Das Gerät ist offline. Bitte beachten Sie, dass **Einstellungen > Onlineprüfung > Prüfe, ob die Geräte online sind** aktiviert sein muss, um den Online-Status anzuzeigen.
	Der UD Pocket zeigt gerade den Anmeldebildschirm (falls konfiguriert).
	Der UD Pocket wird gerade aktualisiert.
	Der UD Pocket ist nicht lizenziert.

Diese und weitere Symbole sowie ihre Bedeutungen finden Sie unter **UMS Konsole > Hilfe > Legende.**

Statusanzeigen, die in der IGEL UMS Web App (see page 783) verwendet werden, finden Sie unter Geräte - Ihre Endgeräte in der IGEL UMS Web App ansehen und verwalten (see page 799).

Gerätebefehle

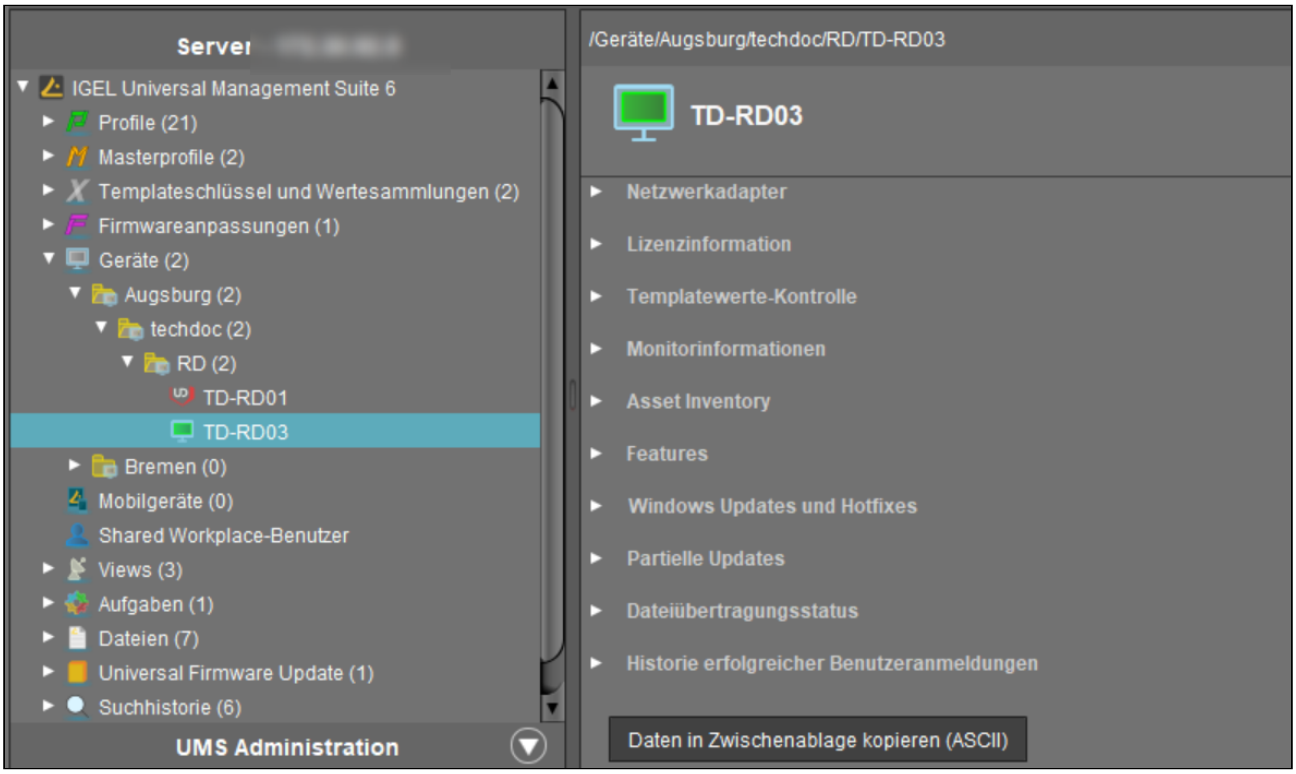
Sie können einen Befehl an ein Gerät über das Kontextmenü (d.h. über einen Rechtsklick auf ein einzelnes Gerät oder ein Geräteverzeichnis) oder über Menüleiste > **Geräte** (see page 343) senden.

- Geräteinformationen in der IGEL UMS einsehen (see page 449)
- Geräte verwalten (see page 455)
- Geräte konfigurieren (see page 464)
- Daten exportieren und importieren (see page 467)
- Nachricht senden (see page 474)
- Sicheres Terminal (Secure Shell) (see page 477)
- Spiegeln - IGEL OS Desktop über VNC beobachten (see page 481)

Geräteinformationen in der IGEL UMS einsehen

Im Bereich **Geräte** der IGEL Universal Management Suite (UMS) können Sie aktuelle Informationen zum ausgewählten Gerät einsehen, z. B. Unit ID, MAC-Adresse, Details zu den verfügbaren Lizenzen, Informationen zu angeschlossenen Monitoren, die Historie erfolgreicher Benutzeranmeldungen usw.
Informationen zur Geräteverwaltung in der IGEL UMS Web App finden Sie unter Devices - View and Manage Your Endpoint Devices in the IGEL UMS Web App.

Menüpfad: **Geräte > [Verzeichnisse] > [Name des Geräts]**



Einzelheiten zu den Symbolen für ein IGEL OS-Gerät finden Sie unter Geräte (see page 447).

▶ Klicken Sie auf die Dreieckssymbole, um Hierachiebenen auf- und zuzuklappen.

▶ Klicken Sie Daten in Zwischenablage kopieren (ASCII), um die Geräteinformationen im ASCII-Format zu kopieren.

Die folgenden Details zum ausgewählten Gerät werden angezeigt:

Systeminformationen

- **Name**

- **Standort**
- **Kommentar**
- **Abteilung**
- **Kostenstelle**
- **Inventarnummer**
- **Inbetriebnahme**
- **Seriennummer**
- **[eigene Attribute]**: Attribute, die unter **UMS Administration > Globale Konfiguration > Geräteattribute** hinzugefügt wurden, werden angezeigt. Für Details, siehe Geräteattribute für IGEL OS Geräte verwalten (see page 593).

Zusätzliche Systeminformationen

- **Unit ID**
- **MAC-Adresse**
- **Letzte IP**
- **Produkt**
- **Produkt-ID**
- **Version**: Version des Betriebssystem
- **Beschreibung der Firmware**
- **Verbunden mit**: Zeigt für ein IGEL OS 12-Gerät an, mit welchem Device Connector es verbunden ist.
- **IGEL Cloud Gateway**
- **Ablaufdatum der OS 10 Maintenance Subscription**
- **Letzter Kontakt**: Der letzte Kontakt zwischen dem Gerät und der UMS. Siehe hier auch Configuring a Device to Send a Heartbeat Signal to the UMS (see page 449).
- **Letzte Startzeit**
- **Netzwerkname beim letzten Neustart**
- **Laufzeit seit letztem Neustart**
- **Laufzeit seit Inbetriebnahme**
- **Batteriezustand**: Bei mobilen Geräten wird der Batteriezustand angezeigt. Die Anzeige wird durch einen Klick auf  aktualisiert. Diese Funktion ist ab IGEL OS 10.03.100 verfügbar. Die Häufigkeit, mit der das Gerät den aktuellen Batteriezustand an die UMS sendet, kann über das Setup eingestellt werden; weitere Informationen finden Sie unter Batteriezustandskontrolle.
- **CPU-Geschwindigkeit (MHz)**
- **CPU-Typ**
- **Größe des Flashspeichers (MB)**
- **Arbeitsspeicher (MB)**
- **Netzwerkgeschwindigkeit**
- **Duplex-Modus**
- **Grafikchipsatz 1**
- **Grafikspeicher 1 (MB)**
- **Grafikchipsatz 2**
- **Grafikspeicher 2 (MB)**
- **Gerätetyp**
- **Betriebssystemtyp**

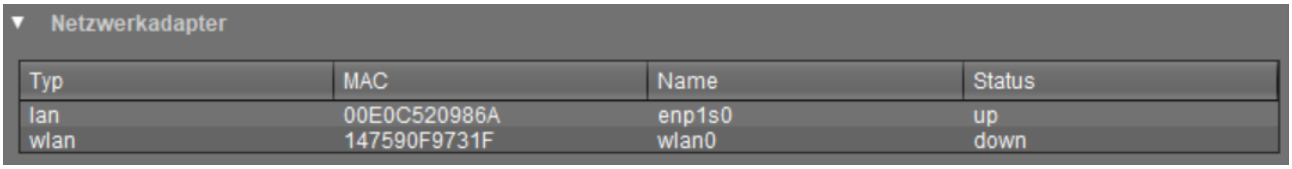
- **BIOS-Hersteller**
- **BIOS-Version**
- **BIOS-Datum**
- **Boot Modus**
- **Seriennummer des Geräts**
- **Strukturtag**. Einzelheiten zu Strukturtags finden Sie unter Verwendung von Struktur-Tags mit IGEL OS 11 Geräten (see page 86).

Netzwerkadapter

In diesem Bereich werden alle verfügbaren Netzwerkadapter eines Geräts aufgelistet. Diese Informationen sind ab IGEL OS 11.07.100 verfügbar.

Die folgenden Informationen zu Netzwerkadaptern werden angezeigt:

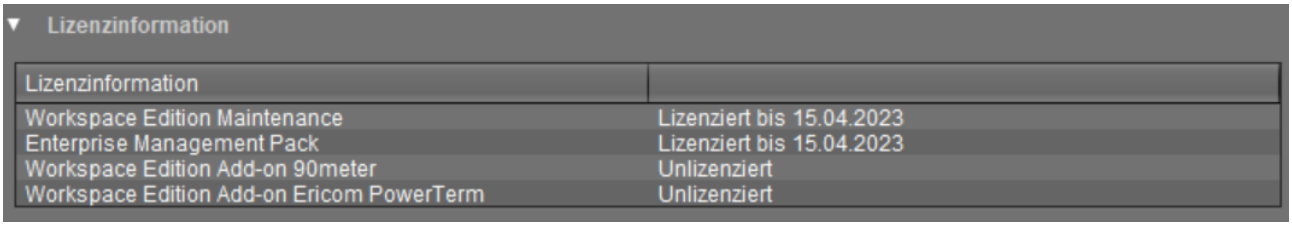
- **Typ**: Typ des Netzwerkadapters
- **MAC**: MAC-Adresse des Netzwerkadapters
- **Name**: Name der entsprechenden Netzwerkschnittstelle
- **Status**: Status des Netzwerkadapters, wie vom Endgerät gesendet, z. B. **down**, **up** (der Netzwerkadapter ist mit einem Netzwerk verbunden, nicht unbedingt mit demselben Netzwerk wie die UMS).



Daten zu Netzwerkadaptern per API auslesen
Sie können Informationen zu Netzwerkadaptern über eine REST-Schnittstelle auslesen. Ausführliche Informationen finden Sie unter Gerät in der IMI API V3 Referenzen.

Lizenzinformationen

In diesem Bereich werden die für das Gerät verfügbaren Lizenzen aufgelistet.

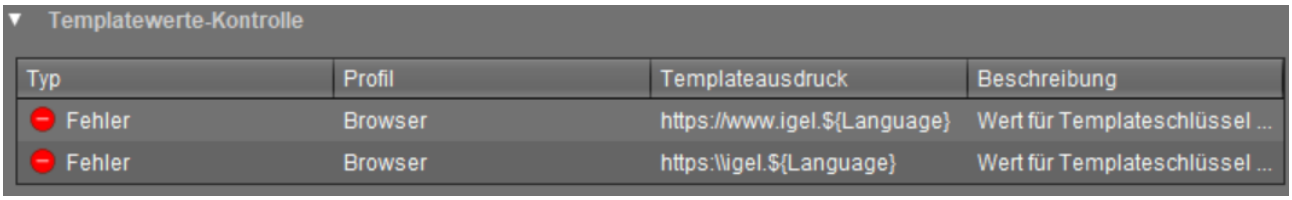


Templatewerte-Kontrolle

In diesem Bereich können Sie die Ergebnisse der Prüfung sehen, ob Templateprofile und Werte korrekt zugewiesen wurden, siehe Templateprofile und Werte den Geräten zuordnen (see page 429). Allgemeine Informationen zu Templateprofilen finden Sie unter Templateprofile in der IGEL UMS (see page 416).

Die folgenden Informationen werden angezeigt.

- **Typ**
- **Profil**
- **Templateausdruck**
- **Beschreibung**



Monitorinformationen

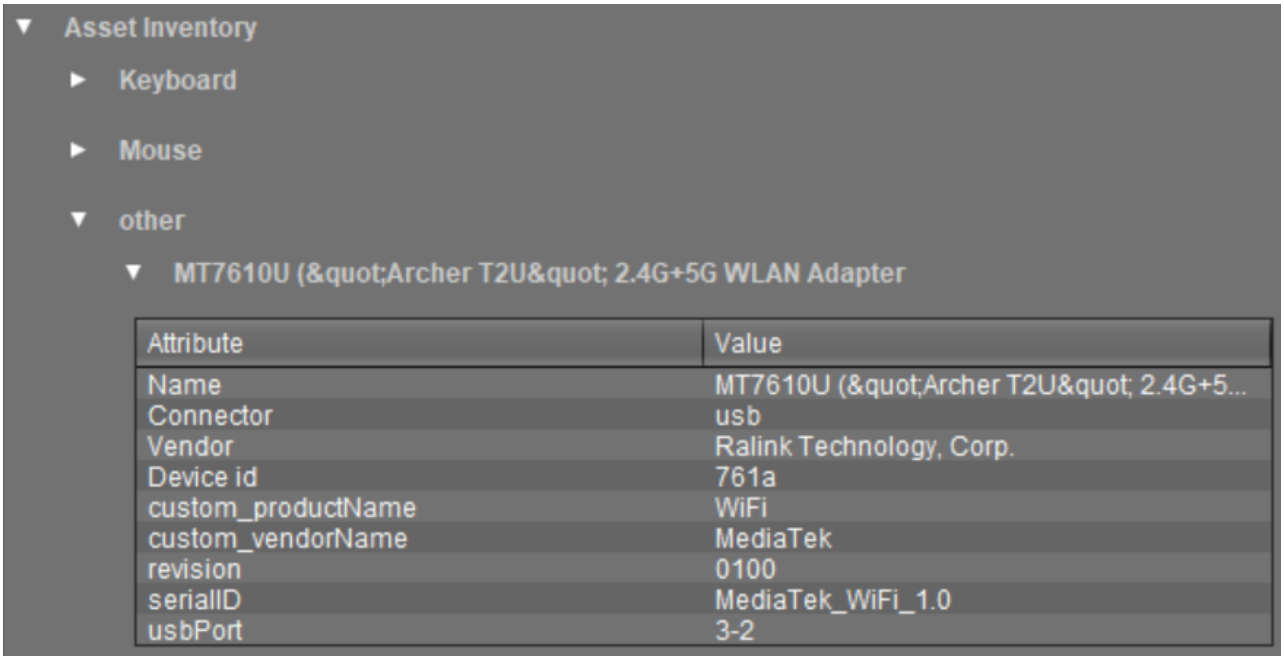
- **Monitor 1**
  - **Hersteller**
  - **Modell**
  - **Seriennumer**
  - **Größe**
  - **Native Auflösung**
  - **Herstellungsdatum**
- **Monitor 2**
  - **Hersteller**
  - **Modell**
  - **Seriennumer**
  - **Größe**
  - **Native Auflösung**
  - **Herstellungsdatum**
- Weitere Monitore, falls anwendbar...

Asset Inventory

> **Lizenz erforderlich**
> Für Geräte mit IGEL OS 11:
> Der Asset Inventory Tracker benötigt eine gültige Lizenz aus dem IGEL Enterprise Management Pack (EMP). Wenn die Lizenz abläuft, ist das Feature nicht mehr verfügbar; Geräte, deren Lizenz abgelaufen ist, senden keine aktuellen Asset-Informationen mehr an die UMS. Informationen zur Bereitstellung von Lizenzen finden Sie unter Automatic License Deployment (ALD) einrichten.
> Für Geräte mit IGEL OS 10:
> Der Asset Inventory Tracker benötigt eine separate Lizenz; wenn die Lizenz abgelaufen ist, aktualisiert die UMS die Asset-Informationen nicht mehr. Informationen zur Bereitstellung von Lizenzen finden Sie unter Licensing AIT.

Mit dieser Funktion erhalten Sie Informationen zu Peripheriegeräten, die an ein Endgerät angeschlossen sind. Die Peripheriegeräte sind nach Kategorien sortiert. Ein Gerät kann mehreren Kategorien zugeordnet sein und dementsprechend mehrfach angezeigt werden.

Der Asset Inventory Tracker kann unter **UMS Administration > Globale Konfiguration > UMS Features > Asset Information anlegen** aktiviert oder deaktiviert werden.



Asset-Daten per API auslesen
Falls Sie eine Lizenz für Asset Inventory Tracker (AIT) besitzen, können Sie Asset-Informationen sowie die Asset-Historie über eine REST-Schnittstelle auslesen. Ausführliche Informationen finden Sie unter Asset Information in der IMI API V3 Referenz.

Features

In diesem Bereich werden die auf dem Gerät verfügbaren Features aufgelistet.

Windows Updates und Hotfixes

In diesem Bereich werden die auf dem Gerät installierten Windows Updates und Hotfixes aufgelistet.

Partielle Updates

In diesem Bereich werden die auf dem Gerät installierten partiellen Updates aufgelistet. Diese Informationen beziehen sich nur auf Windows Geräte, nicht auf IGEL OS-Geräte, und sind ab IGEL Universal Desktop W7 Version 3.12.100 verfügbar.

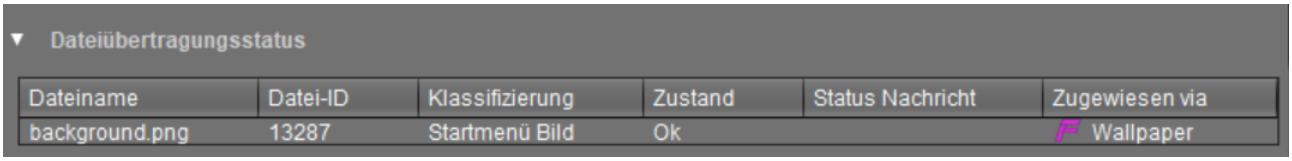
Die folgenden Informationen zu partiellen Updates werden angezeigt:

- **Name**
- **Version**
- **Datum**
- **Beschreibung**

Dateiübertragungsstatus

Ab Firmware IGEL OS 10.05.100 wird hier der Übertragungsstatus bei zugewiesenen Dateien angezeigt, egal, ob sie direkt oder indirekt (über Profile oder Firmwareanpassungen) zugewiesen wurden. Sie erhalten folgende Informationen:

- **Dateiname**
- **Datei-ID**
- **Klassifizierung**: Die Klassifizierung, die beim Hochladen der Datei vergeben wird, oder der Anwendungsfall der Firmwareanpassung oder die Beschreibung des Profils.
- **Zustand** - mögliche Werte:
  - **OK**
  - **Fehler**
  - **unbekannt**
- **Status Nachricht**
- **Zugewiesen via**: Bei direkt zugewiesenen Dateien steht hier der Dateiname, sonst der Name des Profils oder der Firmwareanpassung.



Historie erfolgreicher Benutzeranmeldungen

Benutzeranmeldungen bestimmter Anmeldetypen können in der UMS protokolliert werden.

Die Benutzeranmeldungen werden protokolliert, wenn die folgenden Optionen aktiviert sind:

- Gerät oder Profil: **System > Fernadministration > Optionen >** Kontrollkästchen **Protokolliere Anmelde- und Abmeldeereignisse**
- UMS: **UMS Administration > Zusätzliche Einstellungen >** Kontrollkästchen **Aktiviere die Historie der Benutzeranmeldungen**

Bei aktivierter Protokollierung werden die folgenden Informationen gespeichert:

- **Benutzername**
  Anmeldename des Benutzers, der sich am Client angemeldet hat
- **Zeitstempel der Anmeldung**
  Anmeldezeitpunkt
- **Zeitstempel der Abmeldung**
  Abmeldezeitpunkt
- **Anmeldetyp**
  Die folgenden Anmeldetypen können in der UMS protokolliert werden:
  - **Shared Workplace**
  - **AD/Kerberos**
  - **Citrix**

Geräte verwalten

In der IGEL UMS können Sie Geräte über einen Strukturbaum in Verzeichnisse sortieren. Nutzen Sie die Möglichkeit, um z. B. räumlich oder strukturell zusammengehörige Geräte einfach mit gleichen Profilen versorgen zu können oder um die Geräte entsprechend Ihrer Unternehmensstruktur zu ordnen.

> Aktionen, die auf der Verzeichnisebene durchgeführt werden, gelten für alle Unterverzeichnisse und Geräte, die in diesem Verzeichnis enthalten sind.

- Verzeichnis in der IGEL UMS erstellen (see page 456)
- Geräteverzeichnis kopieren (see page 458)
- Verzeichnis importieren (see page 459)
- Verzeichnis löschen (see page 461)
- Geräte verschieben (see page 462)
- Updates zuweisen (see page 463)

Siehe auch das Video mit einem Überblick darüber, wie man nach Geräten sucht, Verzeichnisse hinzufügt, Geräte in ein Verzeichnis verschiebt und Profile in der IGEL UMS (see page 365) mit Einstellungen für Geräte erstellt:

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=sXw9GW95dgw&list=PLwmmael4krnP_0oALne0k107MHvB9da3B&index=4

Verzeichnis in der IGEL UMS erstellen

In der IGEL Universal Management Suite (UMS) können Sie beliebig viele Verzeichnisse und Unterverzeichnisse erstellen, um die Geräte in Gruppen zusammenzufassen. Wenn Sie Unterverzeichnisse erstellen, bilden die darin organisierten Geräte Untergruppen einer Gruppe.

> Ein Gerät, der durch seine MAC-Adresse eindeutig identifiziert ist, kann nur in einem einzigen Verzeichnis abgelegt sein, also nur Mitglied einer einzigen Gruppe sein.

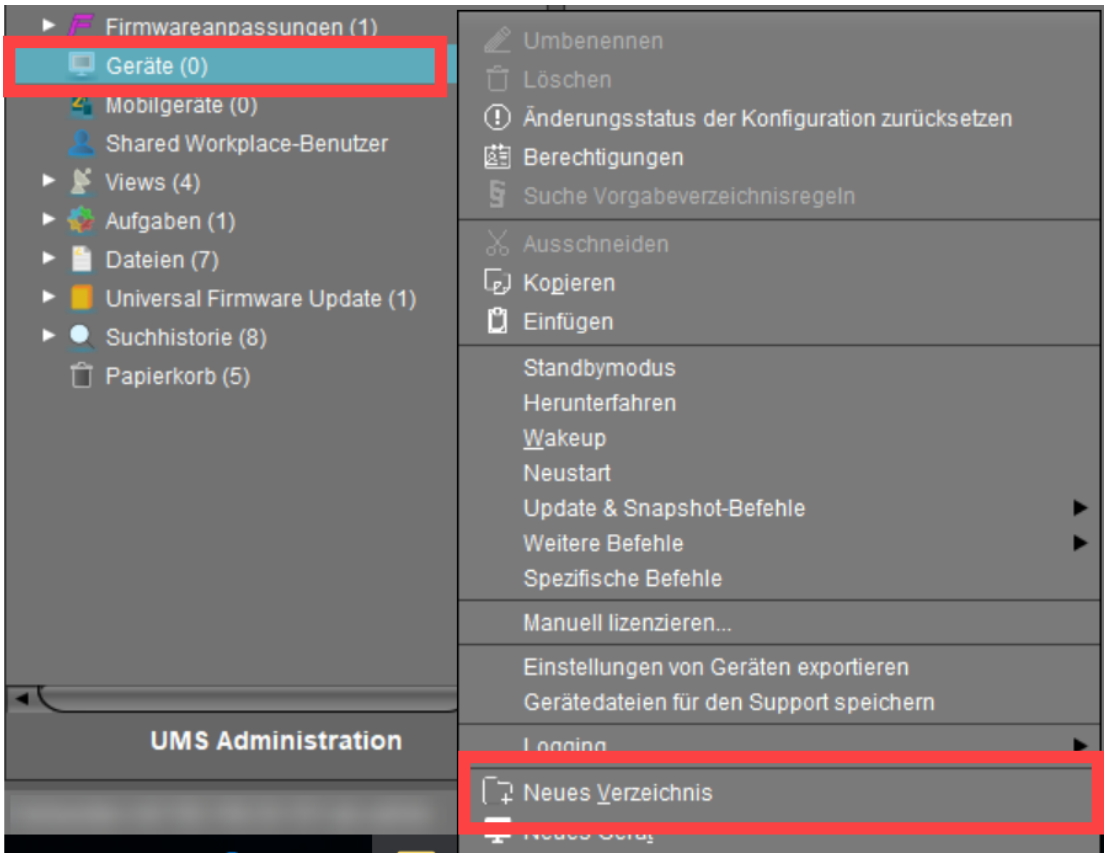
Als Alternative können Sie auch eine Verzeichnisstruktur importieren, siehe Verzeichnis importieren (see page 459).

Informationen zum Erstellen eines Verzeichnisses in der IGEL UMS Web App (see page 783) finden Sie unter Verzeichnisstruktur in der IGEL UMS Web App erstellen (see page 809).

Menüpfad: **UMS Konsole > Geräte**

So erstellen Sie ein Verzeichnis oder Unterverzeichnis:

1. Wählen Sie ein Verzeichnis, z. B. **Geräte**.
2. Wählen Sie aus dem Kontextmenü des ausgewählten Verzeichnisses die Option **Neues Verzeichnis**
   ODER
   Klicken Sie in der Hauptmenüleiste **System > Neu > Neues Verzeichnis**.



3. Geben Sie den **Namen** für das neue Verzeichnis ein. (Max. 100 Zeichen)

4. Klicken Sie **OK**.
   Das neue Verzeichnis wird im Strukturbaum direkt unter dem ausgewählten Verzeichnis angezeigt.

Nun können Sie Geräte in dieses neue Verzeichnis verschieben.

Für das erstellte Verzeichnis können Sie auch Vorgabeverzeichnisregeln definieren, siehe Vorgabeverzeichnisse (see page 643).

Geräteverzeichnis kopieren

Menüpfad: Strukturbaum **> Geräte >** [Name des Gerätverzeichnisses] > Kontextmenü **> Kopieren**

Sie können ein Geräteverzeichnis kopieren und in ein beliebiges Verzeichnis einfügen. Dabei werden nur das leere Verzeichnis sowie darin enthaltene Unterverzeichnisse kopiert; Geräte können nicht kopiert werden.

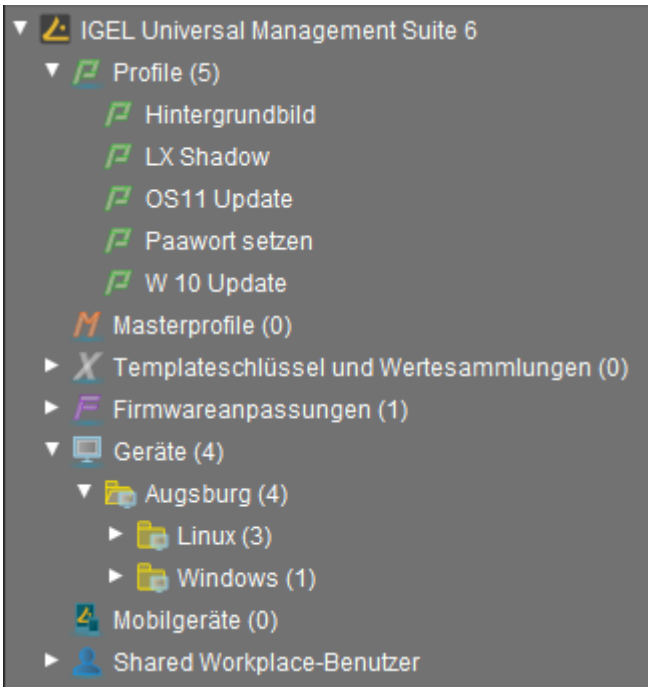
So kopieren Sie ein Geräteverzeichnis:

1. Klicken Sie das Verzeichnis, das Sie kopieren wollen.
2. Öffnen Sie das Kontextmenü des Verzeichnisses und wählen Sie **Kopieren**.
3. Klicken Sie das Verzeichnis, in das Sie die Kopie des Verzeichnisses einfügen wollen. Dies kann auch das Verzeichnis sein, indem sich das ursprüngliche Verzeichnis befindet.
4. Öffnen Sie das Kontextmenü des Verzeichnisses und wählen Sie **Einfügen**.
   Ein neues Geräteverzeichnis wird angelegt, das den gleichen Namen hat wie das ursprüngliche Verzeichnis. Das neue Verzeichnis enthält neu angelegte Kopien der im ursprünglichen Verzeichnis enthaltenen Unterverzeichnisse.

Informationen zum Kopieren eines Verzeichnisses in der IGEL UMS Web App (see page 783) finden Sie unter Geräteverzeichnis in der IGEL UMS Web App kopieren (see page 811).

Verzeichnis importieren

Wenn Sie eine komplexe Verzeichnisstruktur planen, müssen Sie diese nicht schrittweise in der UMS Konsole erstellen. Sie können stattdessen eine `csv`-Datei erstellen, z. B. mit einem Tabellenkalkulationsprogramm, in der Sie die Verzeichnisstruktur bestimmen, und die Struktur aus dieser Liste importieren.



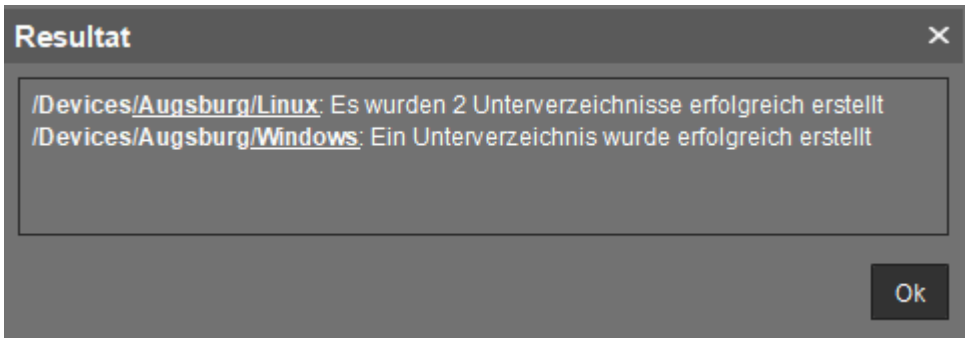
Der oben abgebildeten Baumstruktur liegt folgende Datei zugrunde:

```
Geräte; Augsburg; Linux
```

```
Geräte; Augsburg; Windows
```

So importieren Sie eine Verzeichnisstruktur aus einer `csv`-Datei:

1. Wählen Sie aus dem Hauptmenü **System > Importieren > Verzeichnisse importieren**.
   Das Fenster **Verzeichnisse importieren** öffnet sich.
2. Klicken Sie auf **Datei Öffnen**, um eine `csv`-Datei zu laden.In der ersten Spalte müssen Sie eines der vorgegebenen Stammverzeichnisse festlegen, so können Sie auch Verzeichnisstrukturen für Profile, Aufgaben, Views oder Dateien importieren.
3. Klicken Sie auf **Verzeichnisse importieren**, um die Verzeichnisstruktur zu erstellen.
   Es öffnet sich ein Fenster mit dem Importergebnis. Neu erstellte Verzeichnisse sind dabei unterstrichen.


Resultat
/Devices/Augsburg/Linux: Es wurden 2 Unterverzeichnisse erfolgreich erstellt
/Devices/Augsburg/Windows: Ein Unterverzeichnis wurde erfolgreich erstellt
Ok

Verzeichnis löschen

So löschen Sie ein Verzeichnis:

1. Markieren Sie das zu löschende Verzeichnis.

   > Löschen Sie das Verzeichnis im Strukturbaum und nicht im Inhaltsbereich des Konsolenfensters, da sonst der gesamte Verzeichnispfad mit gelöscht wird.

2. Klicken Sie **Löschen** im Kontextmenü des Verzeichnisses
   oder klicken Sie **Löschen** in der Symbolleiste
   oder drücken Sie die [Entf]-Taste.

   Eine Liste mit allen zu löschenden Objekten wird angezeigt.

   > Wird ein Verzeichnis gelöscht, so werden auch alle darin enthaltenen Unterverzeichnisse und Objekte, wie Geräte, Profile oder Views, gelöscht.

3. Bestätigen Sie den Löschvorgang mit **OK**.

Details zum Löschen von Verzeichnissen in der IGEL UMS Web App (see page 783) finden Sie unter Verzeichnis in der IGEL UMS Web App löschen (see page 814).

Geräte verschieben

Jedes Gerät kann nur einmal im Strukturbaum angezeigt werden. Sie können die Geräte daher nicht kopieren, sondern nur verschieben.

Drag-and-Drop ist die einfachste Möglichkeit, Geräte aus einem Verzeichnis in ein anderes zu verschieben:

1. Halten Sie die [Strg]-Taste gedrückt, wenn Sie mehrere Geräte auswählen möchten.
2. Verwenden Sie die [Umschalt]-Taste, um eine Reihe von Geräten auszuwählen.
3. Bestätigen Sie die Verschiebung mit **Ja**.
   Das Fenster **Änderungszeitpunkt** öffnet sich.

   > Werden dem Gerät durch die Neuzuordnung zu einem Verzeichnis indirekt Profile zugewiesen oder entzogen, so ändert sich seine Konfiguration. Diese wird entweder sofort oder beim nächsten Neustart wirksam.

4. Wählen Sie aus, wann die Änderungen wirksam werden sollen und bestätigen Sie mit **OK**.

Diese beiden Bestätigungsdialoge können Sie im jeweiligen Fenster deaktivieren. Dies lässt sich unter **Extras > Einstellungen > Allgemein** wieder rückgängig machen.

Details zum Verschieben von Geräten in der IGEL UMS Web App (see page 783) finden Sie unter Geräte in der IGEL UMS Web App verschieben (see page 810).

Updates zuweisen

Sie haben mehrere Möglichkeiten, einem Gerät ein registriertes Firmwareupdate zuzuweisen:

- Direkt:
  - mittels Drag & Drop
  - mittels **Zugeordnete Objekte** in der Geräteansicht

- Indirekt:
  - über ein Verzeichnis

> Das Zuordnen eines Firmwareupdates löst den Updateprozess nicht aus. Hierbei wird lediglich die für das Update erforderliche Information an das Gerät übertragen.

> Wenn Sie ein Windows-basiertes Gerät verwenden, lesen Sie die Kapitel Snapshots und Partielles Update im Windows 10 IoT-Handbuch.

Der Updateprozess lässt sich auf zwei Arten starten:

- Manuell:
  a. Klicken Sie mit der rechten Maustaste auf das Gerät im UMS Strukturbaum.
  b. Wählen Sie aus dem Kontextmenü **Update & Snapshot-Befehle > Update** oder **Update beim Herunterfahren**.

- Als Aufgabe:
  a. Klicken Sie mit der rechten Maustaste auf **Aufgaben** im UMS Strukturbaum.
  b. Wählen Sie aus dem Kontextmenü **Neue Aufgabe**.
  c. Geben Sie einen **Namen** ein.
  d. Als **Befehl** wählen Sie **Update**, **Update beim Start** oder **Update beim Herunterfahren**.
  e. Vervollständigen Sie die Einrichtung der Aufgabe, siehe Aufgabenkonfigurationen und Ergebnisse (see page 522).
  f. Ordnen Sie die Aufgabe Geräten oder Verzeichnissen zu, siehe Zuordnung (see page 527).

Geräte konfigurieren

Sie haben folgende Möglichkeiten, ein Gerät über die UMS zu konfigurieren:

1. Über **Strukturbaum > [Kontextmenü des Geräts] > Konfiguration bearbeiten**: Hier können sie das Setup des Clients so bearbeiten, als wenn Sie direkt am Gerät arbeiten würden.
2. Über ein Profil: Über ein Profil weisen Sie dem Client Teilkonfigurationen zu.
3. Über das Spiegeln mit VNC: Indem Sie den Client spiegeln, können Sie direkt im Setup am Gerät arbeiten.

So können Sie die Gerätekonfiguration lokal im Setup des Clients oder auch direkt für diesen Client in der IGEL UMS bearbeiten:

▶ Doppelklicken Sie das Gerät im Strukturbaum
oder wählen Sie **Konfiguration bearbeiten** aus dem Menü / Kontextmenü
oder wählen Sie das entsprechende Symbol aus der Symbolleiste.

Der Konfigurationsdialog eines Geräts in der UMS sowie die Konfiguration eines Profils entsprechen im Aufbau dem lokalen Setup eines Geräts. Details hierzu sind im zugehörigen Handbuch beschrieben.

	Mit Klick auf dieses Symbol können Sie ab UMS Version *5.09.100* Einstellungen wieder auf den Standardwert zurückzusetzen.

Ab UMS Version *5.05.100* enthält die Startseite des Konfigurationsdialogs eine Verknüpfung zur zuletzt geöffneten Seite. Das Symbol  für die Verknüpfung befindet sich ganz oben in der Liste der Verknüpfungen. Eine Verknüpfung wird auch dann angelegt, wenn die zuletzt geöffnete Seite zu einem anderen Gerät bzw. zu einem anderen Profil gehört. Falls die zuletzt geöffnete Seite im aktuell geöffneten Konfigurationsdialog nicht vorhanden ist, wird eine Verknüpfung zur im Strukturbaum nächsthöheren Seite angelegt. Beispiel: Im Konfigurationsdialog für Gerät 1 wurde eine Einstellung für die RDP-Sitzung **Meine RDP-Sitzung** geändert (Menüpfad: **Sitzungen > RDP > RDP-Sitzungen > Meine RDP-Sitzung**). Danach wird der Konfigurationsdialog für Gerät 2 geöffnet, wobei Gerät 2 keine Sitzung mit dem Sitzungsnamen **Meine RDP-Sitzung** hat. Daher wird eine Verknüpfung zur übergeordneten Seite **RDP-Sitzungen** angezeigt (Menüpfad: **Sitzungen > RDP > RDP-Sitzungen**).

So bestimmen Sie, wann die Konfigurationsänderungen wirksam werden sollen:

1. Ändern Sie die Konfiguration.
2. Klicken Sie **Speichern**.
3. Wählen Sie aus, wann die Einstellungen wirksam werden sollen.
   - **Nächster Neustart**: Das Gerät ruft seine Einstellungen bei jedem Start automatisch ab.
   - **Sofort**: Die Einstellungen werden umgehend an das Gerät übertragen.

   Wenn das Gerät nicht in Betrieb ist, kann diese Operation nicht ausgeführt werden, und das Gerät erhält seine Einstellung beim nächsten Neustart. In beiden Fällen werden die Einstellungen zunächst in der Datenbank gespeichert.

Wenn Sie **Sofort** gewählt haben, wird der Benutzer des Geräts in einem Pop-up-Dialog gefragt, ob die neuen Einstellungen sofort wirksam werden sollen. Sie können die Benutzerabfrage ändern mit den beiden Registry-Parametern: `userinterface.rmagent.enable_usermessage` und `userinterface.rmagent.message_timeout`.

Sitzung kopieren

Sie können im Konfigurationsdialog eines Geräts eine Sitzung kopieren. Dabei entsteht ein Duplikat mit allen Eigenschaften der ursprünglichen Sitzung.

So kopieren Sie eine Sitzung:

1. Öffnen Sie den Konfigurationsdialog über **Strukturbaum > Geräte > [Verzeichnis]** mit einem Doppelklick auf das Gerät.
2. Wählen Sie im Konfigurationsdialog **Sitzungen > [Sitzungstyp] > [Sitzungen des Sitzungstyps]**.
   Beispiel: **RDP-Sitzungen**
   Die bereits angelegten Sitzungen werden angezeigt.
3. Markieren Sie die Sitzung, die Sie kopieren wollen.
4. Klicken Sie  .
   Ein Duplikat der ursprünglichen Sitzung wird angelegt und unterhalb eingefügt.

> Ab *UMS Version 5.03.100* können Sie eine Sitzung auch über das Kontextmenü im Strukturbaum der Gerätekonfiguration kopieren.

Daten exportieren und importieren

Sie können Daten für Geräte exportieren und importieren. Die Einstellungen und Parameter werden in einem XML-Format gespeichert.

Firmwares exportieren

Menüpfad: **System > Exportieren > Firmwares exportieren**

Sie können die Daten bestimmter Firmwareversionen exportieren. Die exportierten Daten enthalten alle Einstellungsparameter, die in der UMS sowie im lokalen Setup verfügbar sind.

So exportieren Sie Firmwaredaten:

1. Gehen Sie zu **System** > **Exportieren** > **Firmwares exportieren**.
   Im Fenster **Firmwares exportieren** werden alle verfügbaren Firmwaredaten angezeigt.
2. Wählen Sie in der Spalte **Aufnehmen** die Firmwaredaten, die Sie exportieren wollen.
3. Legen Sie mit **Archiv erstellen** fest, wie die Firmwaredaten gespeichert werden sollen:
   - ☑ Die Firmwaredaten werden als ZIP-Archiv gespeichert.
   - ☐ Jeder Firmwaredatensatz wird in einer eigenen Datei gespeichert.
4. Klicken Sie **Ok** und wählen Sie einen Speicherort aus.
5. Klicken Sie **Speichern**.
   Die Firmwaredaten werden gespeichert.

Firmwares importieren

Menüpfad: **System > Importieren > Firmwares importieren**

Sie können die Konfigurationsdaten für bestimmte Firmwareversionen importieren. Die Firmwaredaten enthalten alle Einstellungsparameter, die in der UMS sowie im lokalen Setup des Geräts verfügbar sind. Diese Firmwaredaten werden für die Erstellung von Profilen und beim Import von Geräten benötigt.

So importieren Sie die Firmwaredaten:

1. Gehen Sie zu **System** > **Importieren** > **Firmwares importieren**.
2. Wählen Sie die Datei mit den Firmwaredaten und klicken Sie **Öffnen**.
   Wenn Sie eine einzelne Datei ausgewählt haben, werden die Firmwaredaten sofort importiert.
3. Wenn Sie ein ZIP-Archiv ausgewählt haben, wählen Sie die zu importierenden Firmwaredaten aus und klicken Sie **Ok**.
   Im Fenster **Ergebnisse** werden die importierten Firmwaredaten angezeigt.

Geräteeinstellungen in der IGEL UMS exportieren

In der IGEL Universal Management Suite (UMS) können Sie die Einstellungen von Geräten exportieren. In der exportierten Datei werden alle geänderten Einstellungen gespeichert, d.h. alle Einstellungen, die von den Standardwerten abweichen, unabhängig davon, ob sie über die UMS Profile oder lokal auf dem Gerät konfiguriert sind.

Das Exportieren von Geräteeinstellungen kann für Supportzwecke notwendig sein (siehe Lokale Konfiguration des IGEL OS Geräts exportieren) oder, zum Beispiel, wenn Sie diese später als Profil importieren möchten (siehe Geräte als Profile importieren (see page 473)) und mithilfe der Funktion zum Vergleich der Profileinstellungen (see page 396) die bestehenden Konfigurationen eines Geräts mit Konfigurationen eines anderen Geräts vergleichen möchten, um die Unterschiede in den Einstellungen herauszufinden.

> ⓘ In der UMS Konsole können Sie die Geräteeinstellungen nur für IGEL OS 11-Geräte exportieren. Wenn Sie die Einstellungen von IGEL OS 12-Geräten exportieren möchten, siehe Geräteeinstellungen als Profil in der IGEL UMS Web App exportieren (see page 826).

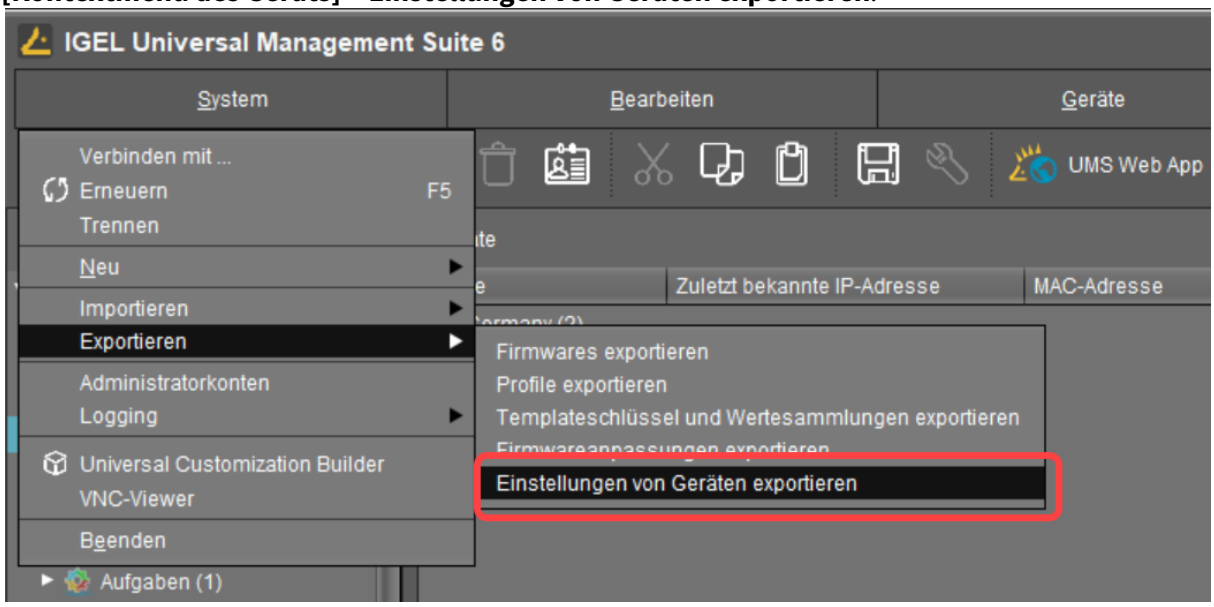
Wenn Sie lediglich Profile exportieren/importieren möchten, siehe Profile exportieren und importieren (see page 390).

Menüpfad: **System > Exportieren > Einstellungen von Geräten exportieren**

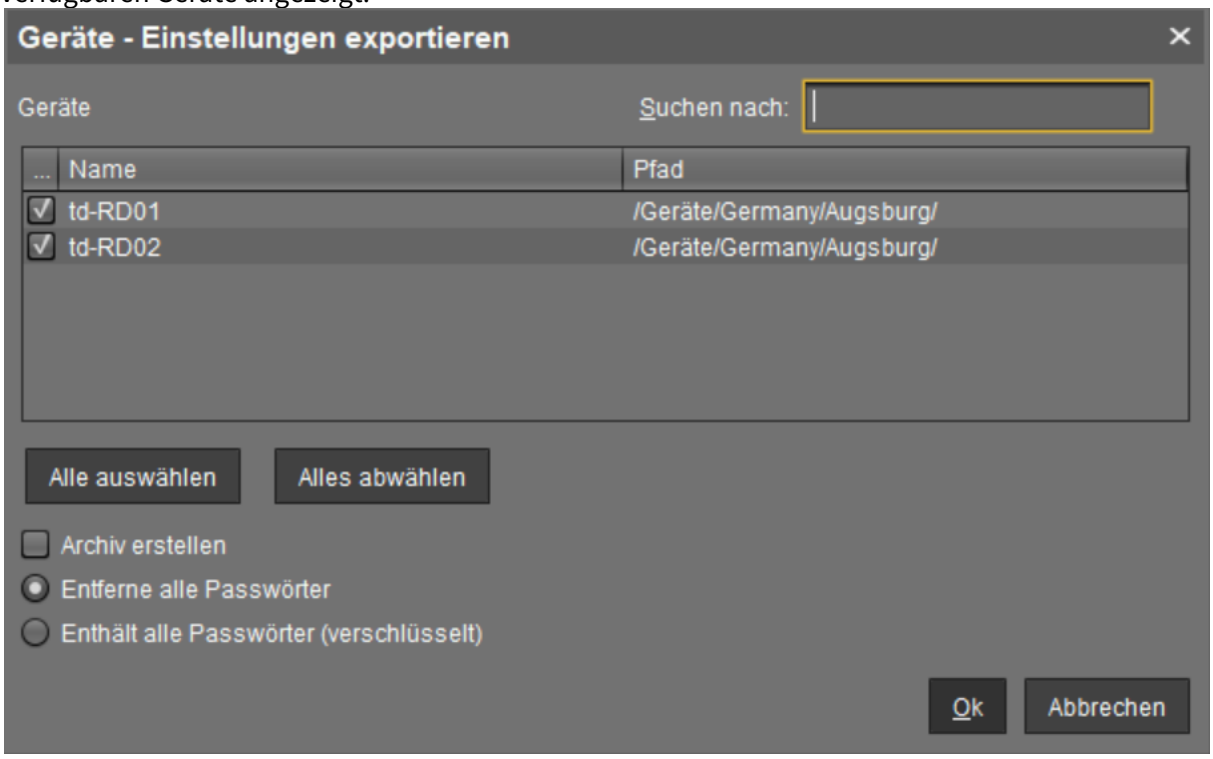
So exportieren Sie die Einstellungen von Geräten:

1. Wenn Sie eine Vorauswahl treffen wollen, markieren Sie in der **UMS Konsole > Geräte** die gewünschten Geräte oder Verzeichnisse.

2. Gehen Sie zu **System > Exportieren > Einstellungen von Geräten exportieren** oder **Geräte > [Kontextmenü des Geräts] > Einstellungen von Geräten exportieren**.



Im Fenster **Geräte - Einstellungen exportieren** werden die zuvor ausgewählten Geräte oder alle verfügbaren Geräte angezeigt.



3. Wählen Sie die Geräte aus, deren Einstellungen Sie exportieren wollen.

4. Legen Sie mit **Archiv erstellen** fest, wie die Einstellungen gespeichert werden sollen:
   ☑ Für jedes Gerät wird eine eigene XML-Datei erzeugt. Die XML-Dateien werden in einem ZIP-Archiv zusammengefasst.
   ☐ Die Einstellungen aller Geräte werden in einer einzigen XML-Datei gespeichert.

5. In UMS 6.10.130 oder höher können Sie bestimmen, ob Passwörter exportiert werden sollen:
   - **Entferne alle Passwörter**: Alle Passwörter werden entfernt, d.h. in der exportierten Datei durch einen Platzhalter ersetzt. (Standard)
     Wenn Sie die exportierten Geräteeinstellungen später als Profil importieren (siehe Geräte als Profile importieren (see page 473)), werden keine Passwörter übernommen. Sie müssen die Passwörter neu setzen.
   - **Enthält alle Passwörter (verschlüsselt)**: Alle Passwörter werden in die exportierte Datei aufgenommen und verschlüsselt.
     Wenn Sie die exportierten Geräteeinstellungen später als Profil importieren, werden alle Passwörter mit importiert und können weiter verwendet werden.

6. Klicken Sie **Ok** und wählen Sie einen Speicherort aus.
7. Klicken Sie **Speichern**.

Geräte als Profile importieren

Menüpfad: **System > Exportieren > Geräte als Profile importieren**

Sie können die Einstellungen von Geräten als Profile importieren. Voraussetzung hierfür ist, dass die Einstellungen mit **System** > **Exportieren** > **Einstellungen von Geräten exportieren** exportiert wurden; siehe Geräteeinstellungen in der IGEL UMS exportieren (see page 470).

So importieren Sie die Einstellungen von Geräten als Profile:

1. Gehen Sie zu **System** > **Importieren** > **Geräte als Profile importieren**.
2. Wählen Sie die Datei mit den Einstellungen und klicken Sie **Öffnen**.
   Das Fenster **Geräte als Profile importieren** öffnet sich.
3. Wählen Sie in der Spalte **Importieren** die zu importierenden Einstellungen aus.
4. Wählen Sie in der Spalte **Firmware (auswählbar)** die Firmware aus, die dem Profil zugrunde liegen soll. (Standard: Die beim Export auf dem Gerät installierte Firmware)
   Die Profile werden im Verzeichnis **Profile** angelegt. Der Namen eines jeden Profils ist identisch mit den Namen des Geräts, von dem die Einstellungen stammen.
   Im Fenster **Ergebnisse** werden aus dem Import erstellten Profile angezeigt.

Nachricht senden

In der IGEL Universal Management Suite (UMS) können Sie an jedes beliebige Gerät eine Nachricht senden. Die Nachricht wird dem Benutzer sofort angezeigt. Nachrichten an Geräte werden unter **UMS Administration > Globale Konfiguration > Nachrichten an Geräte** aktiviert und konfiguriert; siehe Nachrichten an Geräte (see page 666).

Nachrichten an IGEL OS 12-Geräte können auch über die UMS Web App gesendet werden, siehe Eine Nachricht an Geräte über die IGEL UMS Web App senden (see page 820).

Menüpfad: **UMS Konsole > Geräte > [Name des Geräts / Geräteverzeichnisses] > Weitere Befehle > Nachricht senden**

Den Editor starten Sie über das Kontextmenü im **Geräte**-Knoten oder über das Hauptmenü unter **Geräte > Weitere Befehle > Nachricht senden**.

> Formatierte Nachrichten werden auf IGEL OS 11-Geräten angezeigt. Auf IGEL OS 12-Geräten werden die Nachrichten automatisch ohne Formatierung angezeigt, da derzeit nur reine Textnachrichten unterstützt werden.

Unter **Template auswählen** werden Ihnen verschiedene Formatvorlagen zur Auswahl gestellt, darunter voreingestellte Vorlagen und die, die Sie unter **UMS Administration > Globale Konfiguration >** Nachrichten an Geräte (see page 666) angelegt haben:

- {01 template: Info}: Für informative Texte, mit Infosymbol
- {02 template: Warning}: Für warnende Texte, mit Achtungsymbol
- {03 template: Error}: Für Fehlermeldungen, mit Fehlersymbol
- {04 template: Custom Icon}: Frei zu gestaltende Nachricht, mit eigenem Symbol (s.u.)
- {05 template: Alert}: Rote Alarmnachricht, mit Infosymbol und einer Tabelle mit bewegtem Glockensymbol
- {06 template: Blue}: Blaues Nachrichtenfenster, mit IGEL Symbol
- ... eigene Templates ...

Eigenes Symbol

Um ein eigenes Symbol von der UMS aus zu verteilen, wählen Sie eine PNG-Datei aus, die nicht größer als 4 KB sein sollte.

Die Benutzer, die das Recht besitzen, Nachrichten zu versenden, können alle gespeicherten Templates einsehen und diese für eine Sofortnachricht verändern. Die Änderungen werden allerdings nicht gespeichert.

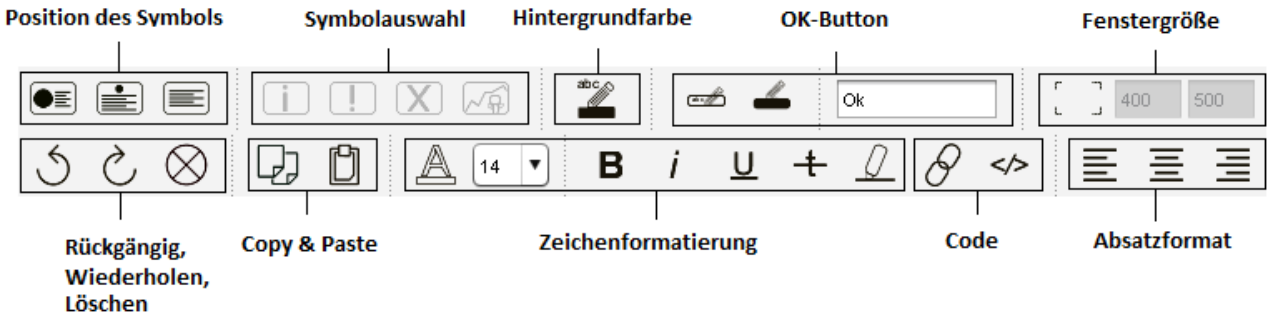
> Um Templates zu speichern, benötigt der Benutzer Schreibrechte auf dem Knoten **UMS Administration > Globale Konfiguration >** Nachrichten an Geräte (see page 666).

Für die Formatierung des Textes können Sie entweder die integrierte Werkzeugleiste nutzen, oder Sie erstellen mit einem Expertentool HTML-Snippets und fügen diese per Copy & Paste ein.

> Eine Nachricht darf aus bis zu 7.000 Zeichen bestehen, einschließlich der Formatierungselemente.

Nachrichteneditor

Menüpfad: **Strukturbaum > Geräte > [Verzeichnisse] > [Name des Geräts] > Weitere Befehle > Nachricht senden**



Sicheres Terminal (Secure Shell)

Sie können eine sichere Terminalverbindung zu einem Gerät herstellen.

Beim Gerät müssen folgende Voraussetzungen erfüllt sein:

- Die Firmware des Geräts ist IGEL Linux v5.11.100 und höher oder IGEL OS 10.01.100 und höher.

> Sie können den Zugriff über das sichere Terminal für alle registrierten Geräte ermöglichen. Aktivieren Sie hierzu die Option **UMS Administration > Globale Konfiguration > Fernzugriff > Sicheres Terminal global aktivieren**.

Für IGEL OS 10.01.100 oder neuer

1. Gehen Sie im IGEL Setup zu **System > Fernzugriff > Sicheres Terminal**.
2. Aktivieren Sie **Sicheres Terminal**.

Für IGEL Linux v5

▶ Im IGEL Setup aktivieren Sie die folgenden Optionen unter **System > Registry**:

- **network > telnetd > enabled > Telnet-Zugriff erlauben**
- **network > telnetd > secure_mode > Sicheres Terminal**

Sicheres Terminal konfigurieren

Mit den folgenden Einstellungen konfigurieren und verwalten Sie den Zugriff auf Geräte über ein sicheres Terminal.

- **Extras > Einstellungen > Fernzugriff > Externer Terminal-Client**: Befehlszeile für den externen Terminal-Client, zusammengesetzt aus dem Pfad zur ausführbaren Datei (z.B. `putty.exe`) und den passenden Parametern. IGEL empfiehlt PuTTY[29].
  Für PuTTY unter MS Windows lautet die minimale Befehlszeile ohne weitere Konfiguration wie folgt:
  `[Pfad und Dateiname für putty.exe] -telnet <hostname> -P <port>`
  Für PuTTY unter Linux lautet die minimale Befehlszeile ohne weitere Konfiguration wie folgt:
  `[Pfad und Dateiname der ausführbaren Datei von PuTTy] -telnet <hostname> -P <port>`

  > `<port>` und `<hostname>` sind Platzhalter, die bei der Ausführung automatisch durch die Portnummer und die IP-Adresse des Geräts ersetzt werden. Hintergrund: Die eigentliche Verbindung zum Gerät wird durch die UMS bereitgestellt und steht dem externen Terminal-Client als Tunnel zur Verfügung.

  Beispiele:
  PuTTy unter MS Windows `C:\Program Files\PuTTY\putty.exe -telnet <hostname> -P <port>`
  PuTTy unter Linux: `/bin/putty - telnet <hostname> -P <port>`
  Wenn das Feld **Externer Terminal-Client** leer ist, wird der interne Terminal-Client der UMS verwendet.
- **Extras > Einstellungen > Fernzugriff > Beendedialog anzeigen, falls zwei oder mehr Sitzungen offen sind**
  ☑ Wenn zwei oder mehrere Sitzungen offen sind, wird beim Versuch, ein Fenster des externen Terminal-Clients zu schließen, ein Beendedialog angezeigt.
  ☐ Beim Schließen des Fensters des externen Terminal-Clients wird kein Beendedialog angezeigt.
- **Extras > Einstellungen > Fernzugriff > Warndialog für unerwartet beendete Sitzungen anzeigen**
  ☑ Wenn eine Sitzung mit einem externen Terminal-Client ohne Zutun des Benutzers beendet wurde, wird ein Warndialog angezeigt.
  ☐ Kein Warndialog wird angezeigt.
- **UMS Administration > Globale Konfiguration > Fernzugriff > Sicheres Terminal global aktivieren**
  ☑ Der Zugriff über das sichere Terminal ist für alle registrierten Geräte aktiviert. Voraussetzung ist, dass die Firmware IGEL Linux v5.11.100 oder höher ist.

29 http://www.chiark.greenend.org.uk/~sgtatham/putty/

☐ Der Zugriff über das sichere Terminal ist nicht für alle registrierten Geräte aktiviert, kann aber für einzelne Geräte aktiviert werden.

- **UMS Administration > Globale Konfiguration > Fernzugriff > Benutzername für sicheres Terminal loggen**: Legt fest, ob der Benutzername des UMS Benutzers protokolliert wird, der die Verbindung zum Gerät hergestellt hat. Das Protokoll wird unter **System > Logging > Fernzugriff** angezeigt.
  ☑ Der Benutzername ist im Protokoll enthalten.
  ☐ Der Benutzername ist nicht im Protokoll enthalten.
- **System > Logging > Fernzugriff-Logs**: Zeigt das Protokoll aller sicheren Zugriffe auf Geräte an. Die folgenden Daten werden protokolliert:
  - **Name des Geräts**
  - **MAC-Adresse**
  - **Unit-ID**
  - **Geräte-IP**
  - **Benutzername**: Benutzername des UMS Benutzers wird protokolliert, der die Verbindung zum Gerät hergestellt hat. Dieser wird nur dann protokolliert, wenn **Benutzername für SSH Fernzugriffe loggen** aktiviert ist.
  - **Startzeit**: Zeitpunkt, zu dem die Verbindung gestartet wurde
  - **Dauer in Sek.**
  - **Kommentar**
  - **Protokoll**: Verbindungsprotokoll

Sicheres Terminal verwenden

So stellen Sie eine sichere Terminalverbindung zu einem Gerät her:

1. Rechtsklicken Sie im Navigationsbaum das Gerät, mit dem Sie sich verbinden wollen.
2. Wählen Sie im Kontextmenü **Sicheres Terminal**.
   Das Terminalfenster öffnet sich. Der Dialog **Sicherheitszertifikat** zeigt das Zertifikat des Geräts an.
3. Klicken Sie **Annehmen**, um das Zertifikat des Geräts zu akzeptieren.
4. Melden Sie sich mit `user` an.

   Die sichere Terminalverbindung zum Gerät ist hergestellt. Sie können zu `root` werden, indem Sie `su` eingeben.

Spiegeln - IGEL OS Desktop über VNC beobachten

Mit der IGEL UMS Konsole können Sie den Desktop eines Geräts durch Spiegeln mit VNC auf Ihrem lokalen PC beobachten.

Um die Spiegelung zu aktivieren, müssen Sie den Fernzugriff für das Gerät zulassen: Wählen Sie im Setup oder Konfigurationsdialog in der UMS **System > Fernzugriff > Spiegeln > Spiegeln des Desktops mit VNC erlauben**.

Für das Spiegeln benötigen Sie **Fernzugriff**-Rechte. Siehe Objektbezogene Zugriffsrechte (see page 687).

Einige Sonderzeichen können möglicherweise nicht über die VNC-Verbindung übertragen werden. Die Verarbeitung von Sonderzeichen hängt von folgenden Faktoren ab:

- Tastaturlayout, das auf dem VNC-Client und dem VNC-Server konfiguriert ist
- Verwendeter VNC Viewer: Ein externer Viewer und der interne Viewer verhalten sich unterschiedlich.
- Firmware-Version des Endgeräts
- UMS Benutzerschnittstelle: Die UMS Konsole und die UMS Web App haben unterschiedliche VNC Viewer.

Für das Spiegeln in der IGEL UMS Web App siehe Fernzugriff auf Geräte über das Spiegeln in der IGEL UMS Web App (see page 824).

IGEL Tech Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=pxwOB8lKyU8

VNC-Sitzung starten

⚠ Einige Sonderzeichen können möglicherweise nicht über die VNC-Verbindung übertragen werden. Die Verarbeitung von Sonderzeichen hängt von folgenden Faktoren ab:

- Tastaturlayout, das auf dem VNC-Client und dem VNC-Server konfiguriert ist
- Verwendeter VNC Viewer: Ein externer Viewer und der interne Viewer verhalten sich unterschiedlich.
- Firmware-Version des Endgeräts
- UMS Benutzerschnittstelle: Die UMS Konsole und die UMS Web App haben unterschiedliche VNC Viewer.

So starten Sie eine VNC-Sitzung:

1. Klicken Sie im Kontextmenü eines Geräts auf **Spiegeln.**
   Ein Verbindungsdialog öffnet sich.
2. Geben Sie das Passwort ein, wenn Sie in den Sicherheitsoptionen ein Passwort festgelegt haben.

Wenn Sie über ein Benutzerkonto verfügen, können Sie sich mit dem UMS-Server verbinden und den IGEL VNC Viewer separat starten. Der IGEL Applikationsordner im Windows-Startmenü enthält einen Link darauf.

1. Geben Sie auf der ersten Registerkarte einen **Hostnamen** oder die **IP-Adresse** manuell ein.
2. Wählen Sie auf der zweiten Registerkarte ein **Gerät** aus dem Strukturbaum aus.

IGEL VNC Viewer

Wenn Sie die VNC-Sitzung gestartet haben, wird der gespiegelte Desktop im Fenster IGEL VNC Viewer angezeigt. Dieses Fenster verfügt über ein eigenes Menü mit den folgenden Elementen:

Datei	**Übersicht**	Zeigt eine Übersicht aller derzeit verbundenen VNC-Sitzungen an. Doppelklicken Sie auf einen der angezeigten Desktops, um ihn in voller Größe darzustellen.
	Beenden	Beendet alle VNC-Sitzungen und schließt das Fenster.
Tab	**Neu**	Öffnet den Verbindungsdialog, sodass Sie eine weitere VNC-Sitzung starten können.
	Anpassen	Mit dieser Option können Sie die Größe des Fensters anpassen, in dem der derzeit ausgewählte Desktop angezeigt wird.
	Strg-Alt-Entf senden	Sendet die Tastenkombination [Strg]+[Alt]+[Entf] an den derzeit angezeigten Remote Host.
	Erneuern	Aktualisiert den Fensterinhalt.
	Screenshot	Schreibt einen Screenshot des Fensterinhalts auf die lokale Festplatte.
	Optionen	Öffnet ein Dialogfenster, in dem Sie weitere Optionen festlegen können, wie Kodierung, Farbtiefe, Aktualisierungsintervall etc.
	Schließen	Schließt die derzeit ausgewählte Registerkarte.
Hilfe / Info		Zeigt die Softwareversion vom IGEL VNC Viewer an.

Folgende Parameter können Sie als Optionen angeben:

Bevorzugte Kodierung	Die für Image-Daten beim Senden vom Gerät zu Ihrem PC verwendete Kodierung. Die Kodierungsoption **Tight** ist besonders in einem Netzwerk mit geringer Bandbreite sinnvoll. Sie beinhaltet zwei zusätzliche Parameter: • **Kompressionsstufe**: Je höher die Komprimierung, umso länger dauert der Rechenvorgang! • **JPEG-Qualität**: Wenn Sie **aus** wählen, werden keine JPEG-Daten versendet.
Zeichne-Rechteck-Methode verwenden	Diese Option verbessert die Leistung. Es können jedoch Artefakte auftreten.
Farbtiefe	8 oder 24 Bit pro Pixel

Aktualisierungsperiode	Zeitspanne zwischen zwei Updates. Eine längere Zeitspanne verringert den Netzwerkverkehr, aber das Update verläuft dann möglicherweise nicht nahtlos. Beachten Sie: Sobald Sie die Maus bewegen oder einen Schlüssel im VNC Viewer eingeben, wird sofort eine Updateanfrage gesendet. Dieses Ereignis wird an den Remote Host weitergegeben.
Eigenschaften als Standard speichern	Speichert die aktuellen Einstellungen als Standardwerte für zukünftige VNC-Sitzungen.

Externe VNC Viewer

⚠ Einige Sonderzeichen können möglicherweise nicht über die VNC-Verbindung übertragen werden. Die Verarbeitung von Sonderzeichen hängt von folgenden Faktoren ab:

- Tastaturlayout, das auf dem VNC-Client und dem VNC-Server konfiguriert ist
- Verwendeter VNC Viewer: Ein externer Viewer und der interne Viewer verhalten sich unterschiedlich.
- Firmware-Version des Endgeräts
- UMS Benutzerschnittstelle: Die UMS Konsole und die UMS Web App haben unterschiedliche VNC Viewer.

Sie können in der UMS Konsole ein externes VNC Viewer-Programm eines anderen Anbieters angeben:

▶ Klicken Sie **Extras > Einstellungen > Fernzugriff**.

Um die IP-Adresse des Geräts an eine externe Anwendung zu übermitteln, fügen Sie in **Externer VNC Viewer** dem Programmaufruf die Parameter `` und `` hinzu.

Beispiele:

- TightVNC: `"C:\Program Files\TightVNC\tvnviewer.exe" <hostname>:<port>`
- UltraVNC: `"C:\Program Files\uvnc\UltraVNC\vncviewer.exe" -connect <hostname>:<port>`
- RealVNC: `"C:\Program Files\RealVNC\VNC Viewer\vncviewer.exe" <hostname>:<port>`
- TigerVNC: `"C:\Program Files\TigerVNC\vncviewer.exe" <hostname>:<port>`

  ⓘ Setzen Sie den Programmpfad wie oben gezeigt in doppelte Anführungszeichen, damit der Aufruf auch trotz Leerzeichen im Pfad funktioniert.

Sicheres Spiegeln (VNC mit SSL/TLS)

In der IGEL Universal Management Suite (UMS) können Sie sicheres VNC für bestimmte Geräte oder global für alle Geräte aktivieren.

Weitere Informationen zum sicheren Spiegeln finden Sie unter Sicheres Spiegeln (VNC mit TLS/SSL).

Menüpfad: **Setup > System > Fernzugriff > Spiegeln > Sichere Verbindung**

Die Funktion **Sicheres Spiegeln** betrifft nur Clients, welche die Voraussetzungen für sicheres Spiegeln erfüllen und die entsprechende Option auch aktiviert haben. Sicheres Spiegeln erhöht die Sicherheit bei der Fernwartung eines Clients über VNC an mehreren Stellen:

- **Verschlüsselung**: Die Verbindung zwischen dem spiegelnden Rechner und dem gespiegelten Client wird verschlüsselt.
  Dies ist unabhängig vom verwendeten VNC Viewer.
- **Integrität**: Nur Clients in der UMS Datenbank können gespiegelt werden.
- **Autorisierung**: Nur autorisierte Personen (UMS Administratoren mit ausreichender Berechtigung) können Clients spiegeln.
  Ein direktes Spiegeln ohne Anmeldung an der UMS ist nicht möglich.
- **Limitierung**: Nur das in der UMS konfigurierte VNC Viewer-Programm (interner oder externer VNC Viewer) kann zum Spiegeln verwendet werden.
  Das direkte Spiegeln eines Clients durch einen anderen Computer wird ebenfalls unterbunden.
- **Protokollierung**: Verbindungen, die über das sichere Spiegeln aufgebaut werden, werden am UMS Server im Log erfasst.
  Zusätzlich zu den Verbindungsdaten lassen sich auch die zugehörigen Benutzerdaten (spiegelnder UMS Administrator, optional) im Log erfassen.

Sicheres Spiegeln aktivieren

So aktivieren Sie sicheres Spiegeln für bestimmte Geräte:

1. Gehen Sie im Konfigurationsdialog oder im IGEL Setup auf **System > Fernzugriff > Spiegeln** und aktivieren Sie **Spiegeln des Desktops mit VNC erlauben**.

2. Aktivieren Sie **Sichere Verbindung** und speichern Sie die Einstellungen.

So aktivieren Sie sicheres Spiegeln global für alle Geräte:

1. Gehen Sie im Konfigurationsdialog oder im IGEL Setup auf **System > Fernzugriff > Spiegeln** und aktivieren Sie **Spiegeln des Desktops mit VNC erlauben**.

2. Aktivieren Sie in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Fernzugriff** die Option **Sicheres VNC global aktivieren**. Siehe Fernzugriff (see page 659).

Sicheres Spiegeln und IGEL OS 12
Das Shadowing von IGEL OS 12-Geräten über die UMS erfolgt immer über das Unified Protocol und ist daher sicher, d. h. die Kommunikation ist immer verschlüsselt. Standardmäßig wird das Shadowing über das einfache VNC-Protokoll verweigert. Sie können jedoch die Option **Spiegeln mittels externen VNC-Tool verbieten** deaktivieren, wenn Sie möchten, dass die Geräte von einem externer VNC Viewer (see page 485) über das einfache VNC-Protokoll beschattet werden können.

Einige Sonderzeichen können möglicherweise nicht über die VNC-Verbindung übertragen werden. Die Verarbeitung von Sonderzeichen hängt von folgenden Faktoren ab:

- Tastaturlayout, das auf dem VNC-Client und dem VNC-Server konfiguriert ist
- Verwendeter VNC Viewer: Ein externer Viewer und der interne Viewer verhalten sich unterschiedlich.
- Firmware-Version des Endgeräts
- UMS Benutzerschnittstelle: Die UMS Konsole und die UMS Web App haben unterschiedliche VNC Viewer.

Shared Workplace-Benutzer

IGEL Shared Workplace ist ein optionales, lizenzpflichtiges Feature der Firmware IGEL OS. Es erlaubt die nutzerabhängige Konfiguration anhand von Profilen, die in der IGEL Universal Management Suite angelegt und mit den AD-Benutzerkonten verknüpft werden. Dabei werden benutzerspezifische Profileinstellungen mit den geräteabhängigen Parametern gemeinsam an das Gerät übermittelt.

Die vollständige Dokumentation finden Sie hier: Shared Workplace (SWP) (see page 951).

Bei der Deaktivierung von **Shared Workplace aktivieren** unter **UMS Administration > Globale Konfiguration > UMS Features** wird der Strukturbaumknoten **Shared Workplace-Benutzer** ausgeblendet. Die Benutzer von Shared Workplace können sich dann NICHT mehr anmelden!

Views

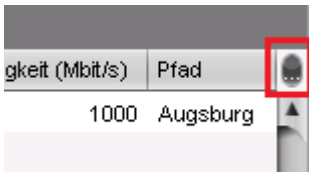
Menüpfad: Strukturbaum **> Views**

Eine View ist eine Auswahl von Geräten nach definierbaren Kriterien, die untereinander logisch verknüpft sind. Sie können Views erstellen, Views bearbeiten oder löschen sowie Ergebnisse einer View in unterschiedlichen Formaten (z. B. XML) exportieren. Diese Baumstruktur kann auch Unterverzeichnisse für die Anordnung von Views beinhalten.

Sie können eine View verwenden, um eine geplante Aufgabe für eine bestimmte Auswahl von Geräten zu definieren, beispielsweise ein Firmwareupdate.

So legen Sie fest, welche Spalten in der View angezeigt werden:

1. Klicken Sie die Auswahl-Schaltfläche in der oberen rechten Ecke des Fensters.



   Der Dialog **Sichtbare Spalten wählen** öffnet sich.

2. Wählen Sie die Spalten aus, die angezeigt werden sollen.

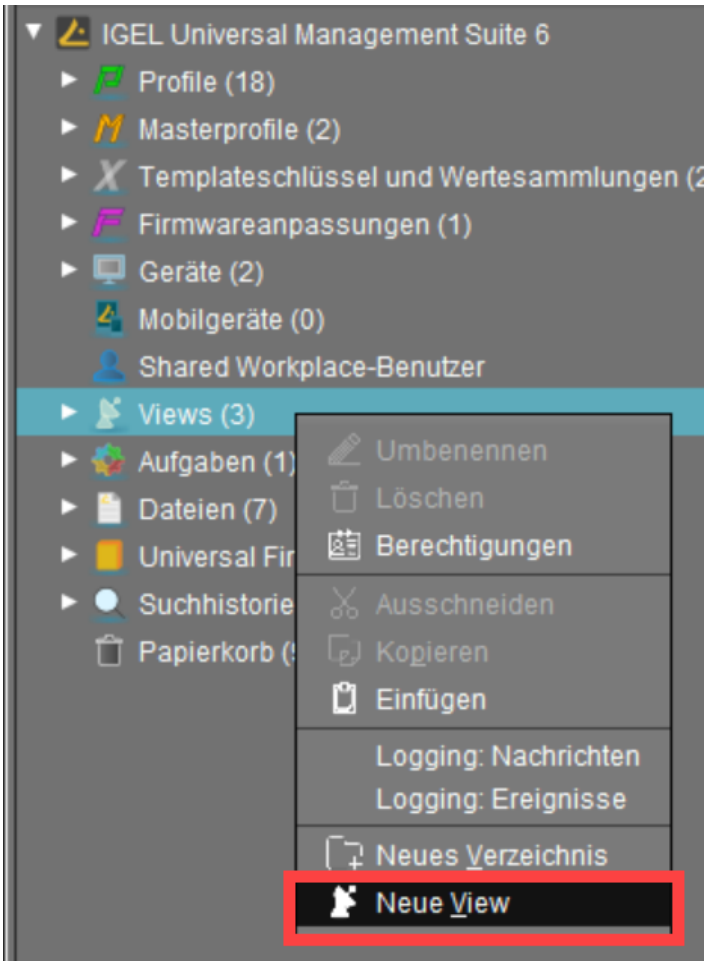
- Wie erstelle ich eine neue View in der IGEL UMS? (see page 490)
- View kopieren (see page 512)
- View-Verzeichnis kopieren (see page 513)
- View-Ergebnisliste speichern (see page 514)
- View per E-Mail verschicken (see page 515)
- Einer View Objekte zuordnen (see page 517)

Wie erstelle ich eine neue View in der IGEL UMS?

Der folgende Artikel beschreibt, wie Sie eine View in der IGEL Universal Management Suite (UMS) erstellen können. Eine View ist eine Auswahl von Geräten nach definierbaren Kriterien, die untereinander logisch verknüpft sind, siehe Views (see page 489). Sie können eine View mit einem Standardverfahren oder mittels Expertenmodus in grafischer / textueller Form erstellen.

Informationen darüber, wie Sie die Anzeige der Ergebnisse von Views konfigurieren können, finden Sie unter Views und Suchen (see page 349).

Menüpfad: **Views > [Kontextmenü] > Neue View**

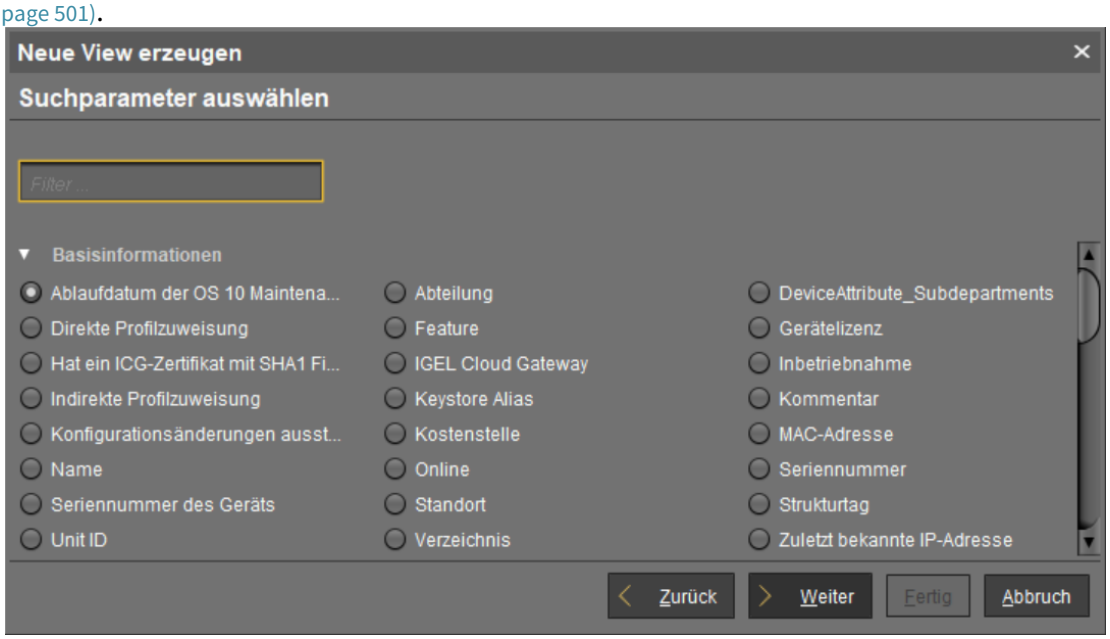


Die Bearbeitung einer View ist nur im Expertenmodus möglich. Um die bereits erstellte View zu ändern, z. B. um weitere Kriterien hinzuzufügen, gehen Sie unter **Views > [Name der View] > [Kontextmenü] > View bearbeiten**.

Eine View erstellen: Standardverfahren

Normalerweise erstellen Sie eine View wie folgt:

1. Gehen Sie in der UMS Konsole auf **Views > [Kontextmenü] > Neue View** oder **System > Neu > Neue View**.
   Das Fenster **Neue View erzeugen** öffnet sich.
2. Vergeben Sie einen **Namen** und eine **Beschreibung**.
3. Klicken Sie **Weiter**.
4. Wählen Sie im Fenster **Suchparameter auswählen** einen Parameter aus.
   Eine Auflistung aller verfügbaren Suchparameter finden Sie unter Mögliche Suchparameter (see page 501).



5. Klicken Sie **Weiter**.
6. Geben Sie im Fenster **Textsuche** in das Eingabefeld den Text ein, mit dem der Parameterwert verglichen werden soll, und wählen Sie eine oder mehrere Suchoptionen.
   Je nach Parameter sind folgende Suchoptionen verfügbar:
   - **Groß-/Kleinschreibung beachten**
     ☑ Die Groß- oder Kleinschreibung des Parameterwerts muss mit der Groß- oder Kleinschreibung im eingegebenen Text übereinstimmen.
     ☐ Die Groß- oder Kleinschreibung des Parameterwerts kann von der Groß- oder Kleinschreibung im eingegebenen Text abweichen.
   - **Ganzen Text vergleichen**
     ☑ Der Parameterwert muss vollständig mit dem eingegebenen Text übereinstimmen.
     ☐ Der Parameterwert muss nicht vollständig mit dem eingegebenen Text übereinstimmen; es genügt, wenn der eingegebene Text im Parameterwert vorkommt.
   - **Regulären Ausdruck verwenden**

☑ Die Optionen **Groß-/Kleinschreibung beachten** und **Ganzen Text vergleichen** sind ausgegraut. Sie können im Eingabefeld einen eigenen regulären Ausdruck eingeben.
Beispiel: `RDD.*` wählt alle Geräte aus, deren Seriennummer die Zeichenkette `RDD` enthält.
Allgemeine Informationen zu regulären Ausdrücken finden Sie z. B. unter Class Pattern[30] in der Oracle-Dokumentation.

☐ Sie können im Eingabefeld keinen regulären Ausdruck eingeben. Bei der nachträglichen Bearbeitung der View jedoch können Sie reguläre Ausdrücken verwenden.

- **Ungleich**
  ☑ Der Parameterwert muss vom eingegebenen Muster abweichen.
  ☐ Der Parameterwert muss mit dem eingegebenen Muster übereinstimmen.
- **Genau**: Der Parameterwert muss mit dem eingegebenen Wert übereinstimmen.
- **Über**: Der Parameterwert muss über dem eingegebenen Wert liegen.
- **Unter**: Der Parameterwert muss unter dem eingegebenen Wert liegen.
- **Ungleich**: Der Parameterwert muss vom eingegebenen Wert abweichen.

7. Klicken Sie **Weiter**.
8. Wählen Sie im Fenster **Erzeugung der View abschließen** eine der folgenden Optionen:
   - **View erzeugen**: Die View wird erzeugt, wenn Sie **Fertig** klicken.
   - **Auswahl weiter einschränken (UND)**: Sie können ein weiteres Auswahlkriterium angeben, das ebenfalls gelten muss. Dieses Auswahlkriterium und das zuvor definierte Auswahlkriterium werden mit einem logischen UND verknüpft.
   - **Auswahl erweitern (ODER)**: Sie können ein weiteres Auswahlkriterium angeben, das alternativ gelten muss. Dieses Auswahlkriterium und das zuvor definierte Auswahlkriterium werden mit einem logischen ODER verknüpft.
9. Klicken Sie je nach ausgewählter Option **Fertig** oder **Weiter**. Sie können beliebig viele Kriterien mit UND/ODER-Verknüpfungen hinzufügen.

Ein Beispiel finden Sie unter Beispiel: View erstellen (see page 504).

Eine View erstellen: Expertenmodus

Sie können eine neue View auch mittels Expertenmodus erstellen – entweder in grafischer Form oder im Textmodus. Es ist möglich, zwischen dem grafischen Modus und dem Textmodus hin und her zu wechseln, solange die eingegebenen Daten in beiden Modi vollständig und gültig sind.

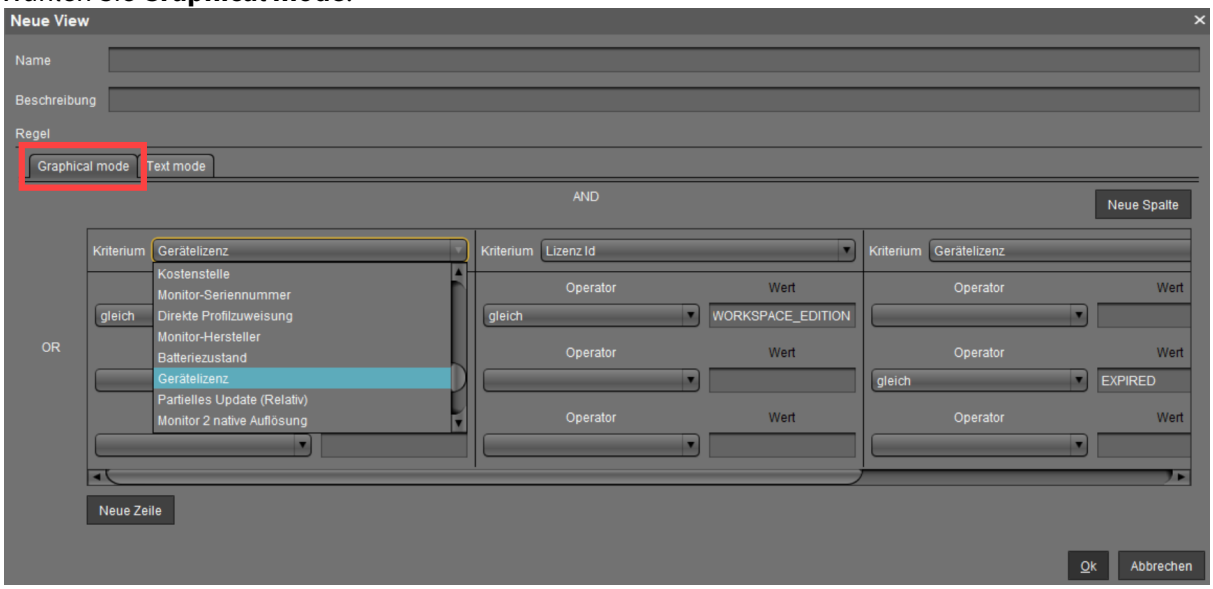
Eine View im grafischen Modus (Graphical Mode) erstellen

Um eine View im grafischen Modus zu erstellen, gehen Sie wie folgt vor:

1. Gehen Sie in der UMS Konsole auf **Views > [Kontextmenü] > Neue View** oder **System > Neu > Neue View**.
   Das Fenster **Neue View erzeugen** öffnet sich.
2. Klicken Sie **Expertenmodus**.
   Das Fenster **Neue View** öffnet sich.

30 https://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html

3. Wählen Sie **Graphical mode**.



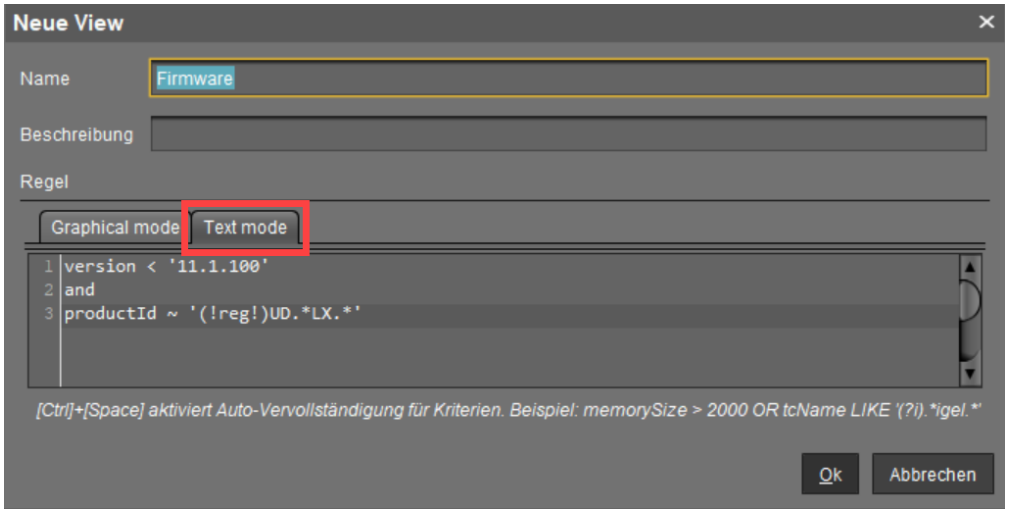
4. Vergeben Sie einen **Namen** und eine **Beschreibung**.
5. Unter **Kriterium** wählen Sie einen Parameter aus.
   Eine Auflistung aller verfügbaren Suchparameter finden Sie unter Mögliche Suchparameter (see page 501).
6. Wählen Sie einen **Operator** aus und definieren Sie den **Wert**. Die Liste der Operatoren kann je nach ausgewähltem Kriterium variieren.
   - **gleich**: Der Parameterwert muss mit dem eingegebenen Wert übereinstimmen.
   - **wie**: Der Parameterwert muss mit dem eingegebenen Muster übereinstimmen.
   - **ungleich**: Der Parameterwert muss vom eingegebenen Muster/Wert abweichen.
   - **kleiner als**: Der Parameterwert muss kleiner sein als der eingegebene Wert.
   - **größer als**: Der Parameterwert muss größer sein als der eingegebene Wert.
7. Klicken Sie **Neue Spalte** / **Neue Zeile**, um weitere Kriterien / Werte zu definieren.
   - Kriterien / Werte in der gleichen Reihe werden mit einem logischen UND verknüpft.
   - Kriterien / Werte in unterschiedlichen Reihen werden mit einem logischen ODER verknüpft.
8. Klicken Sie **Ok**.

Eine View im Textmodus (Text Mode) erstellen

Um eine View im Textmodus zu erstellen, gehen Sie wie folgt vor:

1. Gehen Sie in der UMS Konsole auf **Views > [Kontextmenü] > Neue View** oder **System > Neu > Neue View**.
   Das Fenster **Neue View erzeugen** öffnet sich.
2. Klicken Sie **Expertenmodus**.
   Das Fenster **Neue View** öffnet sich.

3. Wählen Sie **Text mode**.



4. Vergeben Sie einen **Namen** und eine **Beschreibung**.
5. Geben Sie unter **Regel** Ihre Abfrage ein.
   Der Textmodus ermöglicht die Eingabe einer Regel in einer SQL-ähnlichen Abfrage, die aus einem oder mehreren Ausdrücken besteht, siehe Abfragen im Textmodus von Views: Teile eines Ausdrucks (see page 494) unten.
   Sie können die [Eingabetaste] drücken, um von der neuen Zeile aus zu tippen. Zeilenumbrüche können der Bequemlichkeit halber jederzeit eingegeben werden, bleiben aber nicht erhalten, da die Abfrage dynamisch generiert wird, wenn in den Textmodus gewechselt wird.
6. Klicken Sie **Ok**.

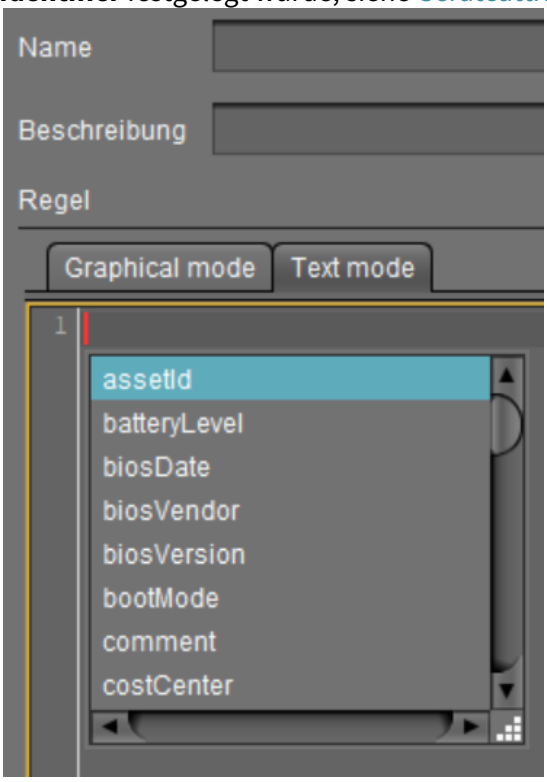
Abfragen im Textmodus von Views: Teile eines Ausdrucks

- Ein Ausdruck besteht aus drei Teilen: KRITERIUM OPERATOR WERT
  Beispiel: `memorySize > 1000`
  Diese Abfrage findet alle Geräte mit einem Systemspeicher größer als 1000 MB.
- Mehrere Ausdrücke können mit den logischen Operatoren `AND` und `OR` verknüpft werden.
  Beachten Sie, dass `AND` Vorrang vor `OR` hat und seine umgebenden Ausdrücke stärker verknüpft.
  Beispiel: `memorySize > 1000 and department = '(?i)sales' or tcName ~ 'Dev.*'`
  Das Suchergebnis dieser Abfrage enthält alle Geräte, die gleichzeitig die Speicher- und Abteilungsbeschränkungen erfüllen und zusätzlich alle Geräte, deren Name mit 'Dev' beginnt.

Kriterium

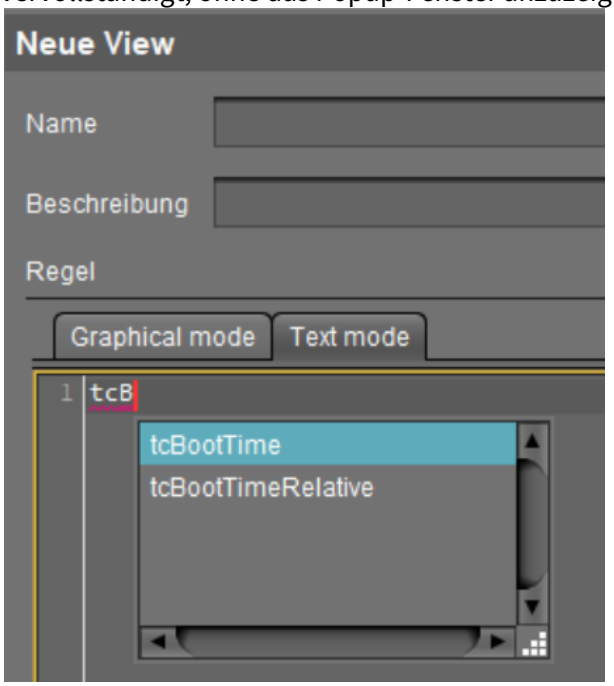
- Mögliche Kriterien und ihre internen Identifikatoren finden Sie unter Textmodus von Views: Matrix der möglichen Kriterien und Operatoren (see page 505).

- [Strg] + [Leertaste] zur Autovervollständigung:
  - Immer wenn ein Kriterium erwartet wird, können Sie [Strg] + [Leertaste] drücken, um die Autovervollständigung zu aktivieren.
    Es öffnet sich ein Popup-Fenster, das alle möglichen Kriterien auflistet. Hier werden auch Geräteattribute über ihre internen Identifikatoren aufgelistet, wenn so ein Identifikator unter **UMS Administration > Globale Konfiguration > Geräteattribute > UMS-interner Identifier** festgelegt wurde, siehe Geräteattribute für IGEL OS Geräte verwalten (see page 593).



  - Die Autovervollständigung funktioniert auch, wenn nur ein Teil des Kriteriums eingegeben wird. Es werden dann nur Kriterien angezeigt, die mit dem bereits eingegebenen Fragment übereinstimmen. Wenn nur ein Kriterium mit dem Fragment übereinstimmt, wird es

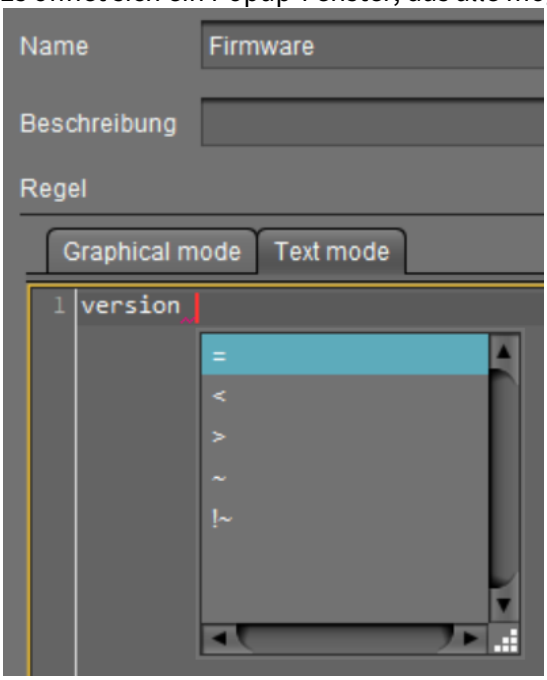
vervollständigt, ohne das Popup-Fenster anzuzeigen.



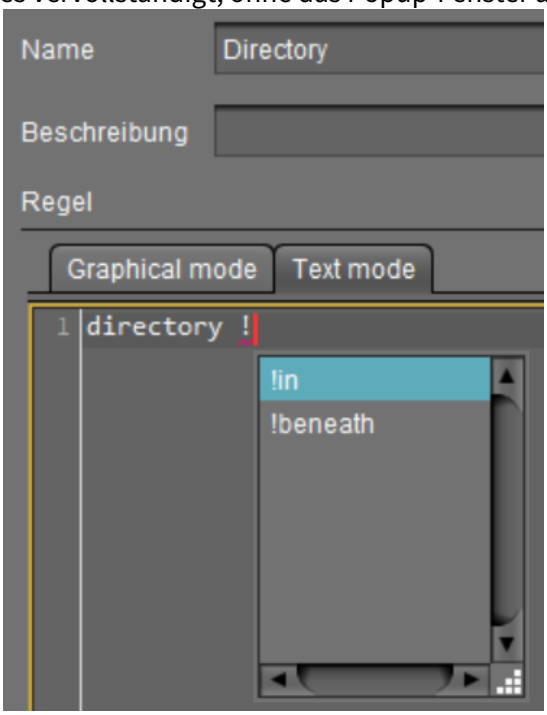
Operator

- Die Liste der Operatoren, die für das eingegebene Kriterium möglich sind, finden Sie unter Textmodus von Views: Matrix der möglichen Kriterien und Operatoren (see page 505).
- [Strg] + [Leertaste] zur Autovervollständigung:
    - Immer wenn ein Operator erwartet wird, d.h. nach einem Kriterium und Leerzeichen, können Sie [Strg] + [Leertaste] drücken, um die Autovervollständigung zu aktivieren.

Es öffnet sich ein Popup-Fenster, das alle möglichen Operatoren auflistet.



- Die Autovervollständigung funktioniert auch, wenn nur ein Teil des Operators eingegeben wird. Es werden dann nur Operatoren angezeigt, die mit dem bereits eingegebenen Fragment übereinstimmen. Wenn nur ein Operator mit dem Fragment übereinstimmt, wird es vervollständigt, ohne das Popup-Fenster anzuzeigen.



- Die möglichen Operatoren sind in der folgenden Tabelle aufgeführt. Die Spalte "Operator" zeigt die Operatornamen, wie sie in den Auswahllisten des grafischen Modus aufgeführt sind.

Der Bequemlichkeit und Lesbarkeit halber werden mehrere Varianten von Operatoren erkannt. Daher kann "LIKE" z. B. auch als "~" geschrieben werden.

Operator	Pattern(s)			
gleich	=			
kleiner als	<			
größer als	>			
wie	~	like	Like	LIKE
ungleich	!~	!like	!Like	!LIKE
in	in	In	IN	
Nicht in	!in	!In	!IN	
unterhalb	beneath	Beneath	BENEATH	
Nicht unterhalb von	!beneath	!Beneath	!BENEATH	
Ist wahr	= true			
Ist falsch	= false			

Wert

- Text- und Datumswerte müssen in doppelte (") oder einfache (') Anführungszeichen gesetzt werden.
- Numerische Werte (integer, dezimale Werte) benötigen keine Anführungszeichen.

Beispiele für Abfragen im Textmodus von Views

Gerätename enthält "igel", wobei `(?i)` ein Flag-Ausdruck für die von Groß- und Kleinschreibung unabhängige Suche ist:

```
tcName LIKE '(?i).*igel.*'
```

Groß- und Kleinschreibung beachten:

```
tcName LIKE '.*IGEL.*'
```

Ganzen Text vergleichen:

```
tcName LIKE '(?i)td-IGEL01'
```

Geräte mit einer bestimmten **Monitorgröße**:

```
monitorSize = 24.1
```

Geräte mit einer bestimmten **letzten Startzeit (Absolut)**:

```
tcBootTime > '2021-05-01' and tcBootTime < '2021-06-25'
```

Geräte mit Geräteattributwerten "KB" oder "KM", wobei `deviceAttributeSubdepartments` ein Identifikator ist, der unter **Geräteattribute > UMS-interner Identifier** angegeben ist, siehe Geräteattribute für IGEL OS Geräte verwalten (see page 593):

```
deviceAttributeSubdepartments ~ 'KB' or deviceAttributeSubdepartments ~ 'KM'
```

Beispiele für reguläre Ausdrücke im Textmodus von Views

Reguläre Ausdrücke werden mittels `(!reg!)` eingeführt. Allgemeine Informationen zu regulären Ausdrücken finden Sie z. B. unter Class Pattern[31] in der Oracle-Dokumentation. Beachten Sie, dass nicht alle dort beschriebenen Konstrukte für reguläre Ausdrücke von der UMS unterstützt werden bzw. ihr Verhalten in der UMS anders sein kann.

- Ein beliebiges Zeichen null oder mehrere Male: `.*`
  Alle Geräte, deren Produkt-ID "UD-LX" enthält, z. B. `UD3-LX51`

  ```
  productId LIKE '(!reg!)UD.*LX.*'
  ```

- Ein beliebiges Zeichen ein oder mehrere Male: `.+`
  Alle Geräte, deren Name nach "igel" ein beliebiges Zeichen ein oder mehrere Male enthält, z. B. `igel1`, `igel203`

  ```
  tcName ~ '(!reg!)igel.+'
  ```

- Ein beliebiges Zeichen einmal oder überhaupt nicht: `.?`
  Alle Geräte, deren Name nach "igel" ein beliebiges Zeichen einmal oder überhaupt nicht enthält, z. B. `igel`, `igel1`

  ```
  tcName like '(!reg!)igel.?'
  ```

- Eine Ziffer [0-9]: `\d`
  Alle Geräte, deren Name nach "igel" eine Ziffer enthält, nach der ein oder mehrere Male ein beliebiges Zeichen folgt, z. B. `igel20`, `igel00E0C520986A`, `igel3DE`

31 https://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html

```
tcName ~ '(!reg!)igel\d.+'
```

- Wertebereich: `[a-zA-Z]`
  Alle Geräte, deren Name nach "igel" eine Hexadezimalzahl (z. B. für MAC-Adressen) ein oder mehrere Male enthält, z. B. `igel00E0C520986A`

```
tcName ~ '(!reg!)igel[0-9A-F]+'
```

Mögliche Suchparameter in der IGEL UMS

Die folgenden Parameter können in der IGEL Universal Management Suite (UMS) als Suchparameter für eine View verwendet werden. Weitere Informationen über Views finden Sie unter Wie erstelle ich eine neue View in der IGEL UMS? (see page 490).

Basisinformationen

- **Ablaufdatum der OS 10 Maintenance Subscription**
- **Abteilung**
- **Direkte Profilzuweisung**
- **Feature**
- **Gerätelizenz**
- **Hat ein ICG-Zertifikat mit SHA1 Fingerprint**
- **IGEL Cloud Gateway**
- **Inbetriebnahme**
- **Indirekte Profilzuweisung**
- **Keystore Alias**
- **Kommentar**
- **Konfigurationsänderungen ausstehend**
- **Kostenstelle**
- **LAN**: Das Endgerät hat mindestens einen LAN-Netzwerkadapter. Siehe den Abschnitt "Netzwerkadapter" unter Geräteinformationen in der IGEL UMS einsehen (see page 449).
- **LAN aktiv**: Das Endgerät ist über einen LAN-Netzwerkadapter mit der UMS verbunden. Siehe den Abschnitt "Netzwerkadapter" unter Geräteinformationen in der IGEL UMS einsehen (see page 449).
- **MAC-Adresse**
- **Name**
- **Online**
- **Seriennummer**
- **Seriennummer des Geräts**
- **Standort**
- **Strukturtag**
- **Unit ID**
- **Verzeichnis**
- **WLAN**: Das Endgerät hat mindestens einen WLAN-Netzwerkadapter. Siehe den Abschnitt "Netzwerkadapter" unter Geräteinformationen in der IGEL UMS einsehen (see page 449).
- **WLAN aktiv**: Das Endgerät ist über einen WLAN-Netzwerkadapter mit der UMS verbunden. Siehe den Abschnitt "Netzwerkadapter" unter Geräteinformationen in der IGEL UMS einsehen (see page 449).
- **Zuletzt bekannte IP-Adresse**
- **[Name des Geräteattributs]**. Details über Geräteattribute finden Sie unter Geräteattribute für IGEL OS Geräte verwalten (see page 593).

Zusätzliche Systeminformationen

- **Arbeitsspeicher**

- **BIOS-Datum**
- **BIOS-Hersteller**
- **BIOS-Version**
- **Batteriezustand**
- **Beschreibung der Firmware**
- **Betriebssystemtyp**
- **Boot-Modus**
- **CPU-Geschwindigkeit**
- **CPU-Typ**
- **Duplex-Modus**
- **Firmwareupdate (Relativ)**
- **Firmwareversion**
- **Flash Player**
- **Flash Player-Version**
- **Flashspeicher**
- **Gerätetyp**
- **Grafikchipsatz 1**
- **Grafikchipsatz 2**
- **Grafikspeicher 1**
- **Grafikspeicher 2**
- **Installierte Apps**: Findet IGEL OS 12-Geräte, auf denen eine bestimmte App / App-Version installiert ist.
- **Inventarnummer**
- **Laufzeit seit Inbetriebnahme**
- **Letzte Startzeit (Absolut)**
- **Letzte Startzeit (Relativ)**
- **Letzter Kontaktzeitpunkt (absolut)** (siehe Configuring a Device to Send a Heartbeat Signal to the UMS (see page 501))
- **Letzter Kontaktzeitpunkt (relativ)** (siehe Configuring a Device to Send a Heartbeat Signal to the UMS (see page 501))
- **Netzwerkgeschwindigkeit**
- **Netzwerkname**
- **Partielles Update (Name)**
- **Partielles Update (Relativ)**
- **Partielles Update (Version)**
- **Produkt**
- **Produkt-ID**

Monitorinformationen

- **Monitor-Hersteller**
- **Monitor-Herstellungsdatum**
- **Monitor-Modell**
- **Monitor-Seriennummer**
- **Monitorgröße**
- **Native Monitorauflösung**

Monitorinformationen (veraltet)

- **Monitor 1 Größe**
- **Monitor 1 Hersteller**
- **Monitor 1 Herstellungsdatum**
- **Monitor 1 Modell**
- **Monitor 1 Seriennummer**
- **Monitor 1 native Auflösung**
- **Monitor 2 Größe**
- **Monitor 2 Hersteller**
- **Monitor 2 Herstellungsdatum**
- **Monitor 2 Modell**
- **Monitor 2 Seriennummer**
- **Monitor 2 native Auflösung**

Beispiel: View erstellen

Menüpfad: **Strukturbaum > Views > Kontextmenü > Neue View**

Im folgenden Beispiel wird eine View erstellt, die alle Geräte mit IGEL OS erfasst, deren Firmwareversion niedriger als 11.01.100 ist. Mit dieser View können Sie feststellen, welche Geräte ein Upgrade erhalten sollten.

1. Klicken Sie im Strukturbaum auf **Views**.
2. Wählen Sie im Kontextmenü **Neue View**.
3. Geben Sie unter **Name** einen passenden Namen für die View ein, etwa `UDLX Update`.
4. Klicken Sie **Weiter**.
5. Wählen Sie im Fenster **Suchparameter auswählen** den Parameter **Firmwareversion**.
6. Klicken Sie **Weiter**.
7. Wählen Sie im Fenster **Versionssuche** bei **Versionsnummer** die Option **Unter** und geben Sie im Textfeld `11.01.100` ein.
8. Klicken Sie **Weiter**.
9. Wählen Sie im Fenster **Erzeugung der View abschließen** die Option **Auswahl weiter einschränken (UND)**.
10. Klicken Sie **Weiter**.
11. Wählen Sie im Fenster **Suchparameter auswählen** den Parameter **Produkt-ID**.
12. Geben Sie im Fenster **Textsuche** den Text `UD.*LX.*` ein und aktivieren Sie **Regulären Ausdruck verwenden**.
13. Klicken Sie **Weiter**.
14. Klicken Sie **Fertig**.
    Das Ergebnis wird im Inhaltsbereich angezeigt. Siehe auch Views und Suchen (see page 349), um mehr über die Optionen für die Anzeige der Ergebnisse von Views zu erfahren.

Textmodus von Views: Matrix der möglichen Kriterien und Operatoren

Kriterium-Name	Interner Identifier	gleich	kleiner als	größer als	wie	ungleich	in	Nicht in	unterhalb	Nicht unterhalb von	Ist wahr	Ist falsch
Ablaufdatum der Lizenz	licenseInfoExpirationDate	x	x	x								
Ablaufdatum der OS 10 Maintenance Subscription	subscriptionExpirationDate	x	x	x								
Abteilung	department	x	x	x	x	x						
Arbeitsspeicher	memorySize		x	x								
BIOS-Datum	biosDate	x	x	x								
BIOS-Hersteller	biosVendor	x	x	x	x	x						
BIOS-Version	biosVersion	x	x	x	x	x						
Batteriezustand	batteryLevel		x	x								
Beschreibung der Firmware	customFirmwarename	x	x	x	x	x						
Betriebssystemtyp	osType	x	x	x	x	x						
Boot-Modus	bootMode	x	x	x	x	x						
CPU-Geschwindigkeit	cpuSpeed		x	x								

Kriterium-Name	Interner Identifier	gleich	kleiner als	größer als	wie	ungleich	in	Nicht in	unterhalb	Nicht unterhalb von	Ist wahr	Ist falsch
CPU-Typ	cpuType	x	x	x	x	x						
Direkte Profilzuweisung	profile2TCAssignment	x				x						
Duplex-Modus	duplexMode	x										
Feature	tcFeature	x				x						
Firmwareupdate (Relativ)	tcFwupdateTimeRelative		x	x								
Firmwareversion	version	x	x	x	x	x						
Flash Player	parameter				x	x						
Flash Player-Version	flashPlayerVersion	x	x	x	x	x						
Flashspeicher	flashSize		x	x								
Gerätelizenz	licenseInfo	x										
Gerätetyp	deviceType	x	x	x	x	x						
Grafikchipsatz 1	graphicsChipset1	x	x	x	x	x						
Grafikchipsatz 2	graphicsChipset2	x	x	x	x	x						
Grafikspeicher 1	graphicsMemorySize1		x	x								
Grafikspeicher 2	graphicsMemorySize2		x	x								

Kriterium-Name	Interner Identifier	gleich	kleiner als	größer als	wie	ungleich	in	Nicht in	unterhalb	Nicht unterhalb von	Ist wahr	Ist falsch
Hat ein ICG-Zertifikat mit SHA1 Fingerprint	usgCertFingerprint	x				x						
IGEL Cloud Gateway	usg										x	x
IGEL Cloud Gateway, zuletzt über ICG gebootet	usgLastBoot										x	x
Inbetriebnahme	inServiceDate	x	x	x	x	x						
Indirekte Profilzuweisung	indProfile2TCAssignment	x				x						
Inventarnummer	assetId	x	x	x	x	x						
Keystore Alias	keystoreAlias	x	x	x	x	x						
Kommentar	comment	x	x	x	x	x						
Konfigurationsänderungen ausstehend	tcConfigChange										x	x
Kostenstelle	costCenter	x	x	x	x	x						
Laufzeit seit Inbetriebnahme	totalUsagetime		x	x								
Letzte Startzeit (Absolut)	tcBootTime	x	x	x								

Kriterium-Name	Interner Identifier	gleich	kleiner als	größer als	wie	ungleich	in	Nicht in	unterhalb	Nicht unterhalb von	Ist wahr	Ist falsch
Letzte Startzeit (Relativ)	tcBootTimeRelative		x	x								
Letzter Kontaktzeitpunkt (absolut)	tcLastContact	x	x	x								
Letzter Kontaktzeitpunkt (relativ)	tcLastContactRelative		x	x								
Lizenz Id	licenseInfoLicenseId	x										
MAC-Adresse	macAddress	x	x	x	x	x						
Monitor 1 Größe	monitor1Size	x	x	x		x						
Monitor 1 Hersteller	monitor1Vendor	x	x	x	x	x						
Monitor 1 Herstellungsdatum	monitor1DateOfProduction	x	x	x	x	x						
Monitor 1 Modell	monitor1Model	x	x	x	x	x						
Monitor 1 Seriennummer	monitor1SerialNumber	x	x	x	x	x						
Monitor 1 native Auflösung	monitor1NativeResolution	x	x	x	x	x						
Monitor 2 Größe	monitor2Size	x	x	x		x						

Kriterium-Name	Interner Identifier	gleich	kleiner als	größer als	wie	ungleich	in	Nicht in	unterhalb	Nicht unterhalb von	Ist wahr	Ist falsch
Monitor 2 Hersteller	monitor2Vendor	x	x	x	x	x						
Monitor 2 Herstellungsdatum	monitor2DateOfProduction	x	x	x	x	x						
Monitor 2 Modell	monitor2Model	x	x	x	x	x						
Monitor 2 Seriennummer	monitor2SerialNumber	x	x	x	x	x						
Monitor 2 native Auflösung	monitor2NativeResolution	x	x	x	x	x						
Monitor-Hersteller	monitorVendor	x	x	x	x	x						
Monitor-Herstellungsdatum	monitorDateOfProduction	x	x	x	x	x						
Monitor-Modell	monitorModel	x	x	x	x	x						
Monitor-Seriennummer	monitorSerialNumber	x	x	x	x	x						
Monitorgröße	monitorSize	x	x	x		x						
Name	tcName	x	x	x	x	x						
Native Monitorauflösung	monitorNativeResolution	x	x	x	x	x						
Netzwerkgeschwindigkeit	networkSpeed		x	x								

Kriterium-Name	Interner Identifier	gleich	kleiner als	größer als	wie	ungleich	in	Nicht in	unterhalb	Nicht unterhalb von	Ist wahr	Ist falsch
Netzwerkname	tcNetworkName	x	x	x	x	x						
Online	online										x	x
Partielles Update (Name)	partialUpdateName	x			x	x						
Partielles Update (Relativ)	partialUpdateTimeRelative		x	x								
Partielles Update (Version)	partialUpdateVersion	x			x	x						
Produkt	model	x	x	x	x	x						
Produkt-ID	productId	x	x	x	x	x						
Seriennummer	serialNumber	x	x	x	x	x						
Seriennummer des Geräts	deviceSerialNumber	x	x	x	x	x						
Standort	site	x	x	x	x	x						
Strukturtag	umsStructuralTag	x	x	x	x	x						
Unit ID	unitId	x	x	x	x	x						
Verzeichnis	directory						x	x	x	x		
Zuletzt bekannte IP-Adresse	ipAddress	x	x	x	x	x						

Kriterium-Name	Interner Identifier	gleich	kleiner als	größer als	wie	ungleich	in	Nicht in	unterhalb	Nicht unterhalb von	Ist wahr	Ist falsch
[Name des Geräteattributs]	Identifikator, der unter **UMS Administration > Globale Konfiguration >** Geräteattribute > UMS-interner Identifier (see page 593) angegeben ist	x	x	x	x	x						

View kopieren

Menüpfad: **Strukturbaum > Views > [Name der View] > Kontextmenü > Kopieren**

Sie können eine View kopieren und in ein beliebiges View-Verzeichnis einfügen.

So kopieren Sie eine View:

1. Klicken Sie die View, die Sie kopieren wollen.
2. Öffnen Sie das Kontextmenü der View und wählen Sie **Kopieren**.
3. Klicken Sie das View-Verzeichnis, in das Sie die Kopie der View einfügen wollen. Dies kann auch das Verzeichnis der ursprünglichen View sein.
4. Öffnen Sie das Kontextmenü des Verzeichnisses und wählen Sie **Einfügen**.
   Eine neue View wird angelegt, die den gleichen Namen sowie die gleichen Eigenschaften hat wie die ursprüngliche View.

View-Verzeichnis kopieren

Menüpfad: **Strukturbaum > Views > [Name des View-Verzeichnisses] > Kontextmenü > Kopieren**

Sie können ein View-Verzeichnis kopieren und in ein beliebiges Verzeichnis einfügen.

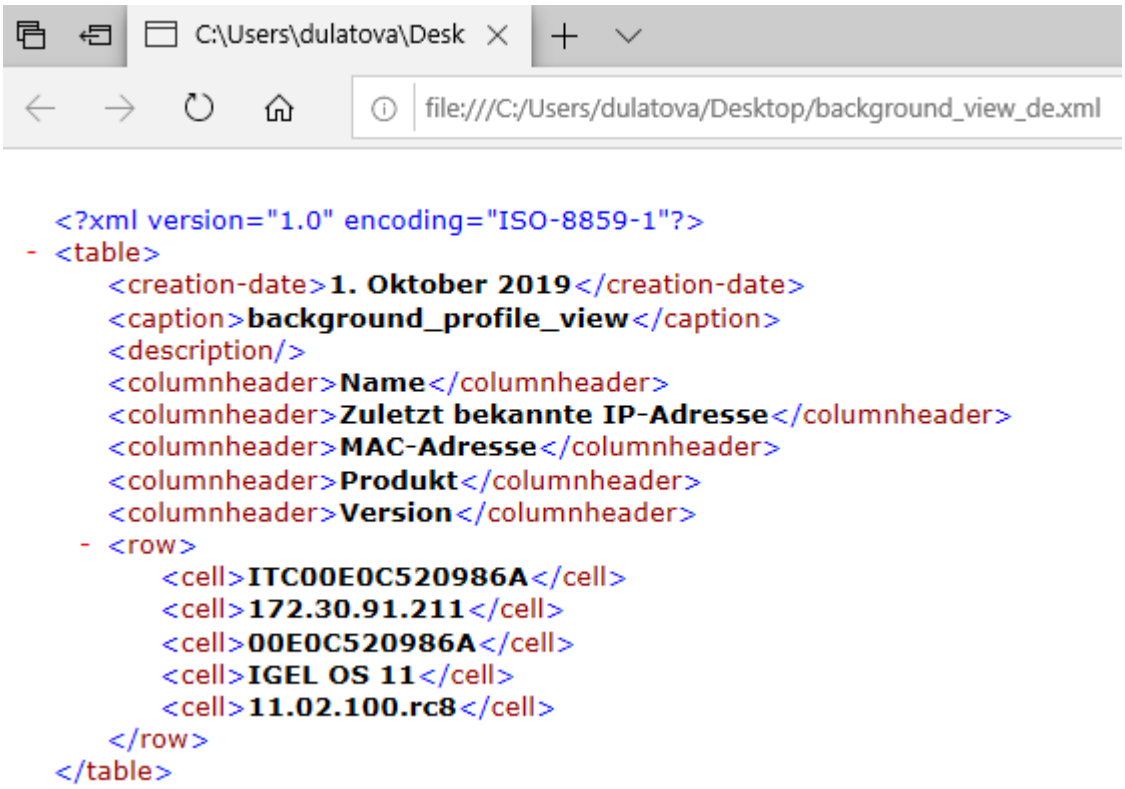
So kopieren Sie ein View-Verzeichnis:

1. Klicken Sie das View-Verzeichnis, das Sie kopieren wollen.
2. Öffnen Sie das Kontextmenü des Verzeichnisses und wählen Sie **Kopieren**.
3. Klicken Sie das Verzeichnis, in das Sie die Kopie des View-Verzeichnisses einfügen wollen. Dies kann auch das Verzeichnis sein, indem sich das ursprüngliche View-Verzeichnis befindet.
4. Öffnen Sie das Kontextmenü des Verzeichnisses und wählen Sie **Einfügen**.
   Ein neues View-Verzeichnis wird angelegt, das den gleichen Namen hat wie das ursprüngliche View-Verzeichnis. Das neue View-Verzeichnis enthält neu angelegte Kopien der im ursprünglichen Verzeichnis enthaltenen Views sowie Kopien der Unterverzeichnisse.

View-Ergebnisliste speichern

▶ Wählen Sie **Speichern unter**... im Kontextmenü einer View, um die aktuelle Ergebnisliste der View in einer Datei zu speichern. Für den Export stehen vier Dateiformate zur Verfügung: XML, HTML, XSL-FO und CSV.

Beispiel für eine XML-Datei einer View:



Die Option **Speichern unter...** ist im Kontextmenü immer dann aktiv, wenn **Automatisch Anzahl und Objekte laden** unter **Menüleiste > Extras > Einstellungen > Views und Suchen > Seitenverhalten > Wenn eine View geladen wird...** ausgewählt wird. Wird dort einer der anderen Parameter ausgewählt, ist die Option **Speichern unter...** erst dann aktiv, wenn eine Schaltfläche **Geräte laden** (oder **Nach Treffern suchen > Geräte laden**) im Inhaltsbereich der View angeklickt wird. Siehe auch Views und Suchen (see page 349).

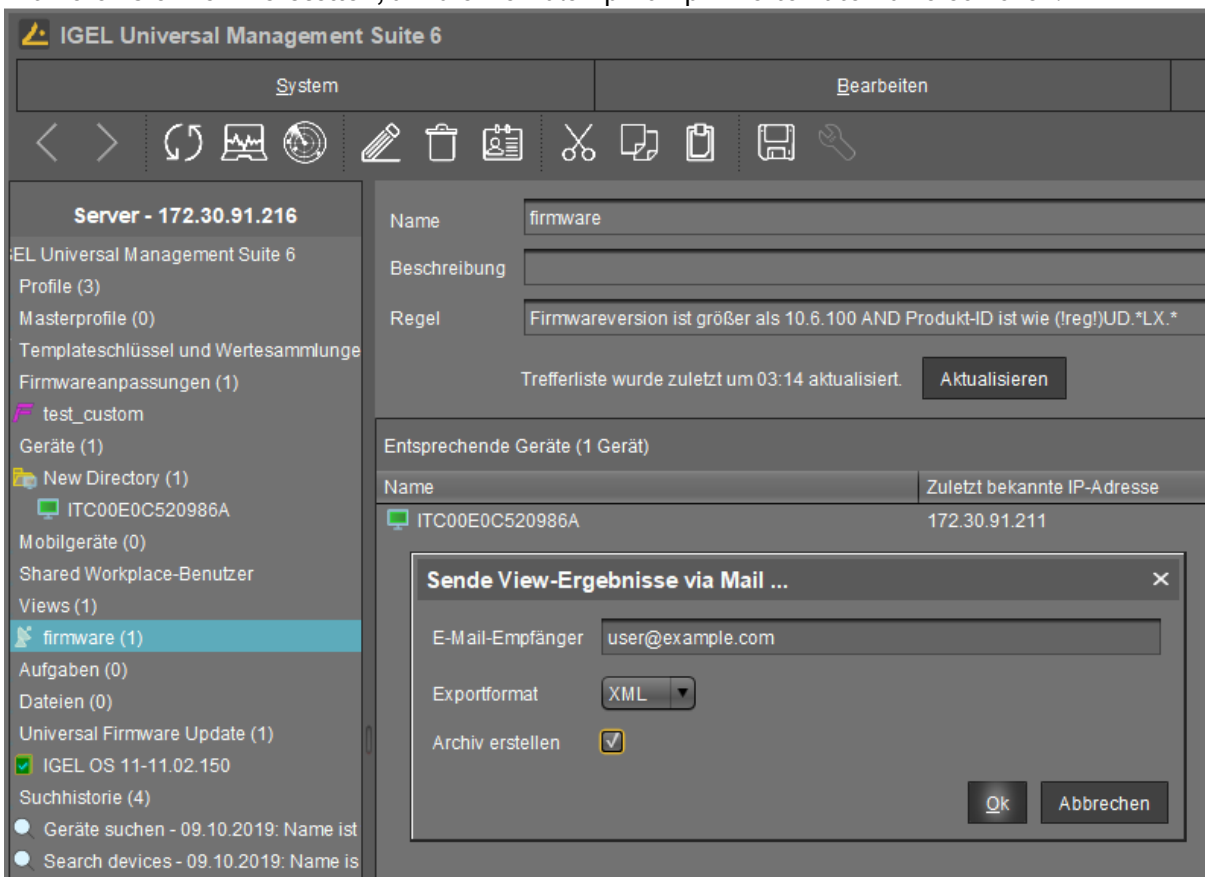
View per E-Mail verschicken

Das Verschicken von E-Mails funktioniert nur, wenn Sie geeignete E-Mail-Einstellungen (see page 664) unter **UMS Administration > Globale Konfiguration > E-Mail-Einstellungen** vorgenommen haben.

So verschicken Sie eine View per E-Mail:

1. Klicken Sie mit der rechten Maustaste auf eine View.
2. Wählen Sie im Kontextmenü **Sende View-Ergebnisse via Mail...** .
   Das Fenster **Sende View-Ergebnisse via Mail...** öffnet sich.

3. Tragen Sie im Feld **E-Mail-Empfänger** die Empfängeradresse ein. Mehrere Empfängeradressen sind möglich, trennen Sie sie mit einem Semikolon ";" von einander.
4. Wählen Sie unter **Exportformat** das Format, in dem die View verschickt werden soll.
5. Aktivieren Sie **Archiv erstellen**, um die View als zip-komprimierte Datei zu verschicken.



Sie können Views auch automatisiert und regelmäßig als Administrative Aufgabe (see page 621) versenden.

Einer View Objekte zuordnen

Sie können Geräten, die Sie über eine View gefiltert haben, über das Kontextmenü der View einmalig Objekte zuweisen. Wenn Sie sicher gehen wollen, dass auch neu erfasste Geräte, die das View-Kriterium erfüllen, das Objekt zugeordnet bekommen, können Sie das über eine Administrative Aufgabe (see page 627) regeln.

> Nach gleichem Schema können Sie auch Geräten Objekte zuweisen, die Sie über eine Suche (see page 543)gefiltert haben.

So weisen Sie einem View-Ergebnis ein Objekt zu:

1. Erstellen Sie eine entsprechende View.
2. Rechtsklicken Sie die View, um das Kontextmenü zu öffnen.
3. Wählen Sie **Objekte zu den Geräten der View zuordnen...** .
   Das Fenster **Objekte zuweisen** öffnet sich.
4. Wählen Sie aus der linken Spalte das gewünschte Objekt und schieben Sie es mit  nach rechts in **Selektierte Objekte**.
5. Klicken Sie **OK**.
   Das Fenster **Änderungszeitpunkt** öffnet sich.
6. Wählen Sie aus, ob die Änderungen **Beim nächsten Neustart** oder **Sofort** wirksam werden sollen.
7. Klicken Sie **OK**.

> Über **Objekte von den Geräten der View entfernen...** können Sie die Zuweisung wieder rückgängig machen.

> Die Optionen **Objekte zu den Geräten der View zuordnen...** und **Objekte von den Geräten der View entfernen...** sind im Kontextmenü der View immer dann aktiv, wenn **Automatisch Anzahl und Objekte laden** unter **Menüleiste > Extras > Einstellungen > Views und Suchen > Seitenverhalten > Wenn eine View geladen wird...** ausgewählt wird. Wird dort einer der anderen Parameter ausgewählt, sind die oben genannten Optionen erst dann aktiv, wenn eine Schaltfläche **Geräte laden** (oder **Nach Treffern suchen > Geräte laden**) im Inhaltsbereich der View angeklickt wird. Siehe auch Views und Suchen (see page 349).

Aufgaben - Senden von automatisierten Befehlen an Geräte in der IGEL UMS

Sie können Aufgaben für die IGEL Universal Management Suite (UMS) definieren. Eine Aufgabe besteht darin, einen Befehl für bestimmte Geräte automatisch zu einer definierten Zeit abzusenden. Aufgaben können in Intervallen oder an bestimmten Wochentagen wiederholt werden.

Menüpfad: **UMS Konsole > Aufgaben**

Im Kontextmenü zu einer Aufgabe haben Sie die folgenden Optionen:

- **Aufgabe bearbeiten**: Öffnet den Dialog **Aufgabe bearbeiten**, mit dem Sie Einstellungen der Aufgabe ändern können.
- **Umbenennen**: Öffnet den Dialog **Eingabe**, indem Sie der Aufgabe einen neuen Namen geben können.
- **Löschen**: Entfernt die Aufgabe.
- **Veraltete Ergebnisse löschen**: Entfernt alte Ergebnisse.
- **Berechtigungen**: Öffnet den Dialog **Berechtigungen** mit dem Sie die Rechte für die Aufgabe ändern können. Weitere Informationen finden Sie unter Objektbezogene Zugriffsrechte (see page 687).
- **Ausschneiden**: Schneidet die Aufgabe aus dem aktuellen Verzeichnis aus, so dass sie in einem anderen Verzeichnis eingefügt werden kann.
- **Einfügen**: Fügt die ausgeschnittene Aufgabe in das aktuelle Verzeichnis ein.
- **Logging: Nachrichten**: Öffnet den Dialog **Nachrichten**. Weitere Informationen finden Sie unter Benutzeraktionen protokollieren (see page 694).
- **Aufgabe ausführen**: Führt die Aufgabe sofort aus.

IGEL Tech Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=F7NI4PDBUMM

Neue Aufgabe anlegen

Sie können in der UMS Konsole Aufträge einrichten, um eine Auswahl von Geräten zu verwalten, indem Sie geplante Befehle an sie senden.

Menüpfad: Strukturbaum > **Aufgaben**

So erstellen Sie einen Auftrag:

1. Wählen Sie **Aufgaben** > [Kontextmenü] > **Neue Aufgabe** oder **System** > **Neu** > **Neue Aufgabe**.
   Der Konfigurationsdialog wird geöffnet. Die in diesem Dialogfeld konfigurierten Parameter können später durch Bearbeiten der Aufgaben geändert werden.

2. Geben Sie unter **Details** die grundlegenden Informationen zu Ihrer Aufgabe und den auszuführenden Befehl an. Weitere Informationen zu den Parametern finden Sie unter "Details" im Viewing Job Configurations and Execution Results (see page 522) und Befehle für Aufgaben (see page 520).

3. Unter **Zeitplan** können Sie die Ausführungszeit weiter anpassen. Weitere Informationen zu den Parametern finden Sie unter "Zeitplan" in Viewing Job Configurations and Execution Results (see page 522).

4. Unter **Zuweisbare Objekte auswählen** können Sie Ihre Aufgabe Geräten, Geräteordnern, Views und Suchen zuweisen. Sie können das Objekt auch später zuweisen. Weitere Informationen finden Sie unter Assigning Objects to a Job (see page 527).
   Sie können auch in der UMS Web App erstellte Advanced Searches zuweisen. Weitere Informationen finden Sie unter Suche nach Geräten in der IGEL UMS Web App (see page 792).

5. Klicken Sie auf **Fertig**, um den Job zu speichern.

Befehle für Aufgaben

Hier finden Sie Information über die Befehle die für eine Aufgabe definiert werden können.

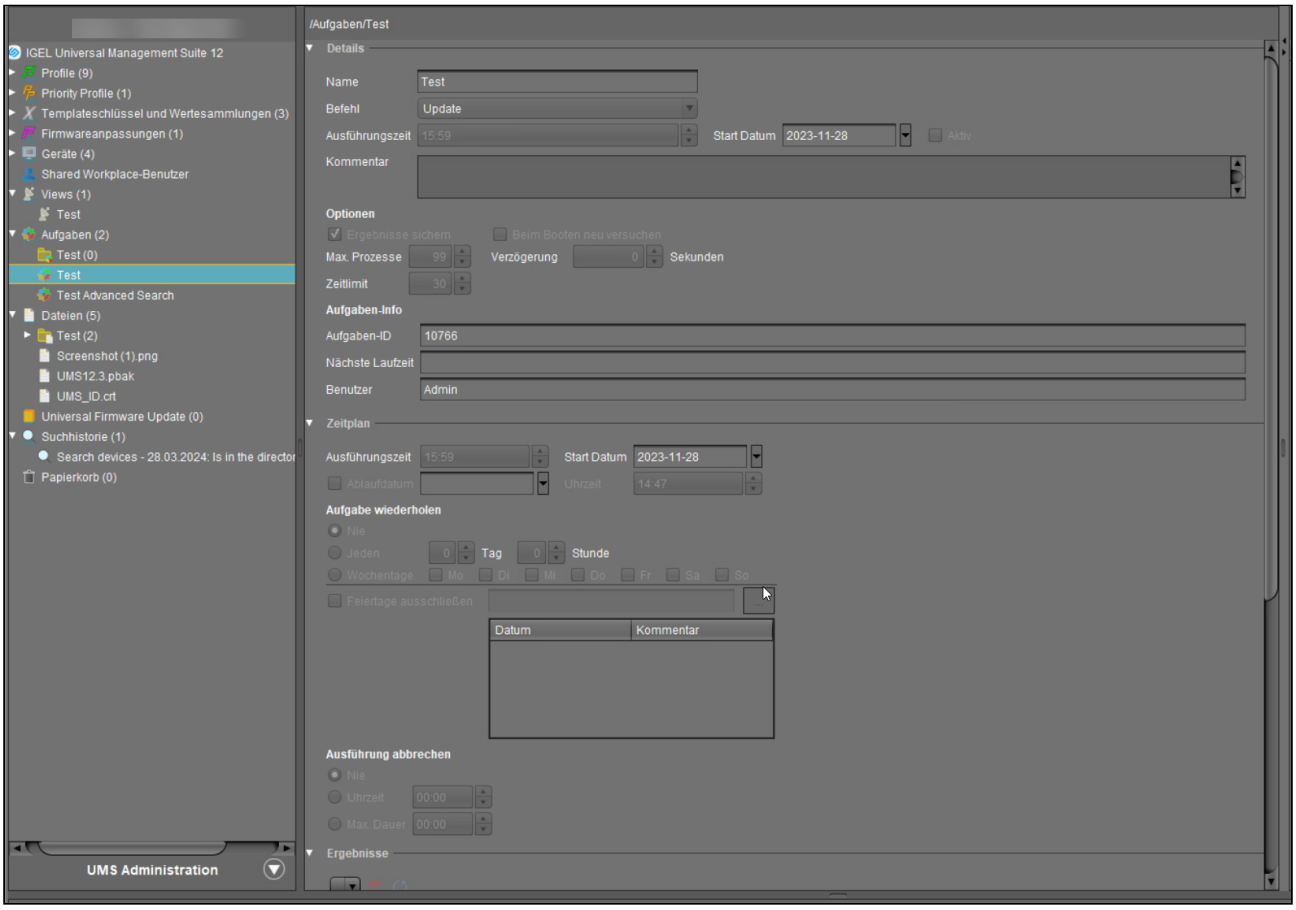
- **Update**
  - IGEL OS 12: Löst die Aktivierung der zugewiesenen App-Version bei den IGEL OS 12-Geräten aus. Der **Update**-Befehl wird nur benötigt, wenn **System > Update > App nach der Installation aktivieren** deaktiviert ist; siehe How to Configure the Background App Update in the IGEL UMS Web App (see page 893).
  - IGEL OS 11 oder früher: Führt das Firmwareupdate mit den bestehenden Einstellungen aus, siehe auch Universal Firmware Update (1) (see page 520).
- **Herunterfahren**: Fährt das Gerät herunter.
- **Neustart**: Startet das Gerät neu.
- **Standbymodus**: Versetzt das Gerät in den Standbymodus.
- **Wakeup**: Startet das Gerät über das Netzwerk (Wake-on-LAN).
- **Update beim Start**: Führt das Firmwareupdate beim Start des Geräts aus (IGEL OS 11 oder früher).
- **Update beim Herunterfahren**: Führt das Firmwareupdate beim Herunterfahren des Geräts aus (IGEL OS 11 oder früher).
- **Einstellungen Gerät->UMS**: Liest die lokalen Einstellungen des Geräts in die UMS ein.
- **Einstellungen UMS->Gerät**: Sendet die lokalen Einstellungen der UMS an das Gerät.
- **Flash Player herunterladen**: Lädt das Flash Player-Plugin für Firefox herunter.
- **Flash Player entfernen**: Entfernt das Flash Player-Plugin für Firefox.
- **Firmware-Snapshot herunterladen**: Führt das Firmwareupdate mit den bestehenden Einstellungen aus (WES).
- **Nachricht senden**: Sendet ein ausgewähltes Nachrichtentemplate an die Geräte. Sie können Templates für Nachrichten unter **UMS Administration > Globale Konfiguration > Nachrichten an Geräte** erstellen. Für weitere Informationen über Nachrichtentemplates, siehe Nachricht senden (see page 474).
- **Partielles Update**: Führt das Partielle Update mit den bestehenden Einstellungen aus (WES). Siehe auch Partielles Update.
- **Desktopanpassungen aktualisieren**: Aktualisiert den Bildschirmhintergrund und das Bootlogo.
- **BIOS - Get settings**: Holt die aktuellen BIOS-Einstellungen vom Gerät. Dieses Kommando wird von den BIOS Tools for Selected HP Devices verwendet.
- **BIOS - Set password**: Setzt ein Passwort für das BIOS. Dieses Kommando wird von den BIOS Tools for Selected HP Devices verwendet.
- **BIOS - Set settings**: Macht die geändeten BIOS-Einstellungen auf dem Gerät wirksam. Dieses Kommando wird von den BIOS Tools for Selected HP Devices verwendet. Dieses wird vom BIOS Update for Devices Supported by LVFS und von den BIOS Tools for Selected HP Devices verwendet.
- **BIOS - Trigger update**: Löst eine Aktualisierung des BIOS aus.
- **Installiere Jabra Xpress Paket**: Installiert ein Jabra Xpress Paket (IGEL OS).
- **OS 11 Upgrade**: Aktualisiert Geräte von IGEL OS 10 auf IGEL OS 11. Siehe Massenbereitstellung über eine geplante Aufgabe.

- **Start Login Enterprise Launcher**: Startet den bereits konfigurierten Login PI Launcher, siehe Login Enterprise Launcher in IGEL OS.

Aufgabenkonfigurationen und Ergebnisse

Hier finden Sie unter **Details** und **Zeitplan** alle für den Aufgabe definierten Parameter. Sie können auch die **Ergebnisse** für einen abgeschlossenen Aufgabe überprüfen.

Menüpfad: Strukturbaum **> Aufgaben >** [Spezifischer Job]



Details

Name

Name der Aufgabe.

Befehl

Befehl, der für alle zugewiesenen Geräte ausgeführt wird. Weitere Informationen finden Sie unter Befehle für Aufgaben (see page 520).

Ausführungszeit / Start Datum

Zeitpunkt der ersten Ausführung

Aktiv

☑ Aufgaben lassen sich nach Bedarf aktivieren oder aussetzen.

Kommentar

Weitere Informationen zur Aufgabe.

Optionen

Ergebnisse sichern

☑ Protokollierbare Ergebnisse werden in der Datenbank erfasst, dies ist nicht möglich für den Befehl `Wake-on-LAN`.

Beim Booten neu versuchen

☑ Parameter für den Updatebefehl – ausgeschaltete Geräte führen das Update beim nächsten Start durch.

Max. Prozesse

Maximale Anzahl gleichzeitig ausgeführter Prozesse, diese werden somit ggf. blockweise ausgeführt.

Verzögerung

Wartezeit, die minimal vergeht, bis die UMS den Befehl an das nächste Gerät verschickt.

Zeitlimit

Wartezeit, die maximal vergeht, bis die UMS den Befehl an das nächste Gerät verschickt.

> ⓘ Die Optionen **Max. Prozesse, Verzögerung** und **Zeitlimit** sind für alle Befehle sinnvoll, deren Ausführung länger dauert oder starken Netzwerkverkehr verursacht, z. B. das Herunterladen eines Firmwareupdates, eines Codecs oder eines Snapshots. Um zu verhindern, dass viele Geräte gleichzeitig Daten von einem Dateiserver herunterladen, wird empfohlen, die Anzahl gleichzeitiger Prozesse zu reduzieren (z. B. auf 10) und eine Verzögerung (z. B. 1 Minute) einzurichten.

Aufgaben-Info

Aufgaben-ID

Interne Aufgabennummer, die nicht bearbeitet werden kann. Bei einer neuen Aufgabe ist dieses Feld leer.

Nächste Laufzeit

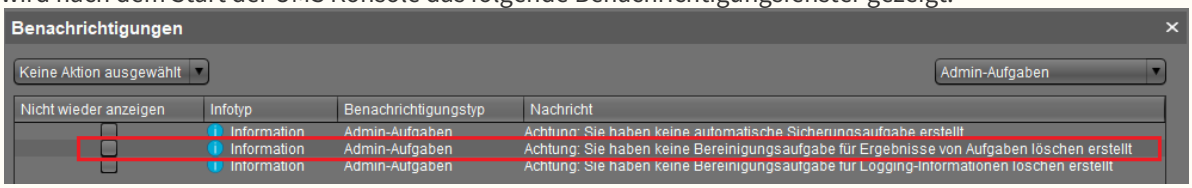
Datum und Uhrzeit der nächsten Ausführung.

Benutzer

Name des UMS Benutzers, der den Befehl ausführt.

Benachrichtigungen für Admin-Aufgaben

Falls Sie keine administrative Aufgabe "Ergebnisse von Aufgaben löschen (see page 609)" angelegt haben, wird nach dem Start der UMS Konsole das folgende Benachrichtigungsfenster gezeigt:



Diese Benachrichtigung können nur Benutzer mit den Leserechten für administrative Aufgaben sehen. Die Rechte können unter **Bearbeiten > Berechtigungen** definiert werden.
Anzeigeeinstellungen können unter **Extras > Einstellungen > Benachrichtigungen** angepasst werden.
Benachrichtigungen sind unter **Hilfe > Benachrichtigungen** zu finden.

Zeitplan

Ausführungszeit/Start Datum

Zeitpunkt der ersten Ausführung.

Ablaufdatum/Uhrzeit

Nach diesem Zeitpunkt werden keine weiteren Befehle ausgeführt.

Aufgabe wiederholen

Eine Aufgabe kann in festen Intervallen oder an bestimmten Tagen wiederholt werden. Feiertage lassen sich gesondert ausschließen. Die Liste der Feiertage pflegen Sie unter **Extras > Geplante Aufgaben > Feiertagslisten verwalten**.

Wenn als Befehl die Aufgabe **Update**, **Update beim Start** oder **Update beim Herunterfahren** ausgewählt ist, sollte **Aufgabe wiederholen** nicht aktiviert sein.

Ausführung abbrechen

Legt fest, wie lange es dauern darf, bis die Ausführung der Aufgabe beendet ist.
Mögliche Optionen:

- **Nie**: Aufgaben werden nie abgebrochen.
- **Uhrzeit**: Zeitpunkt in Stunden und Minuten, zu dem die Ausführung abgebrochen wird.
  Beispiel: Wenn **Ausführungszeit** auf "19:00" und **Ausführung abbrechen** auf "20:00" eingestellt sind, beträgt das Zeitlimit für die Ausführung der Aufgabe 1 Stunde. Nach 20:00 Uhr werden keine weiteren Befehle für die Ausführung der Aufgabe an Geräte verschickt.

  > Liegt die unter **Ausführung abbrechen** eingestellte **Uhrzeit** vor der **Ausführungszeit**, wird die Aufgabenausführung nicht abgebrochen.

- **Max. Dauer**: Wartezeit in Stunden und Minuten, die maximal vergehen darf, bis die Ausführung der Aufgabe beendet ist.
  Beispiel: Wenn **Max. Dauer** auf "00:05" konfiguriert ist, wird maximal 5 Minuten auf die Beendigung der Aufgabenausführung gewartet. Nach 5 Minuten ab **Ausführungszeit** werden keine weiteren Befehle für die Ausführung der Aufgabe an Geräte verschickt.

Ergebnisse

In der Ansicht einer fertig erstellten Aufgabe werden **Ergebnisse** angezeigt. Hier erhalten Sie eine Übersicht der Status für Aufgabenausführungen, aus der Sie über eine Auswahlliste wählen können. Diese Ergebnisansicht lässt sich über zwei Schaltflächen löschen und aktualisieren. Folgende Statusmeldungen der Aufgabe -**Nachricht-** werden für die zugeordneten Geräte erfasst:

Wird ausgeführt	Die Aufgabe wird gerade ausgeführt.
OK	Die Aufgabe ist fertig gestellt, alle zugewiesenen Geräte wurden bearbeitet.
Zeit abgelaufen	Die Aufgabe wurde abgebrochen, bevor alle zugewiesenen Geräte bearbeitet wurden, weil die Abbruchzeit oder die maximale Dauer erreicht worden sind.
Abgebrochen	Die Aufgabe wurde aus unbekannten Gründen angehalten (z. B. Serverausfall).

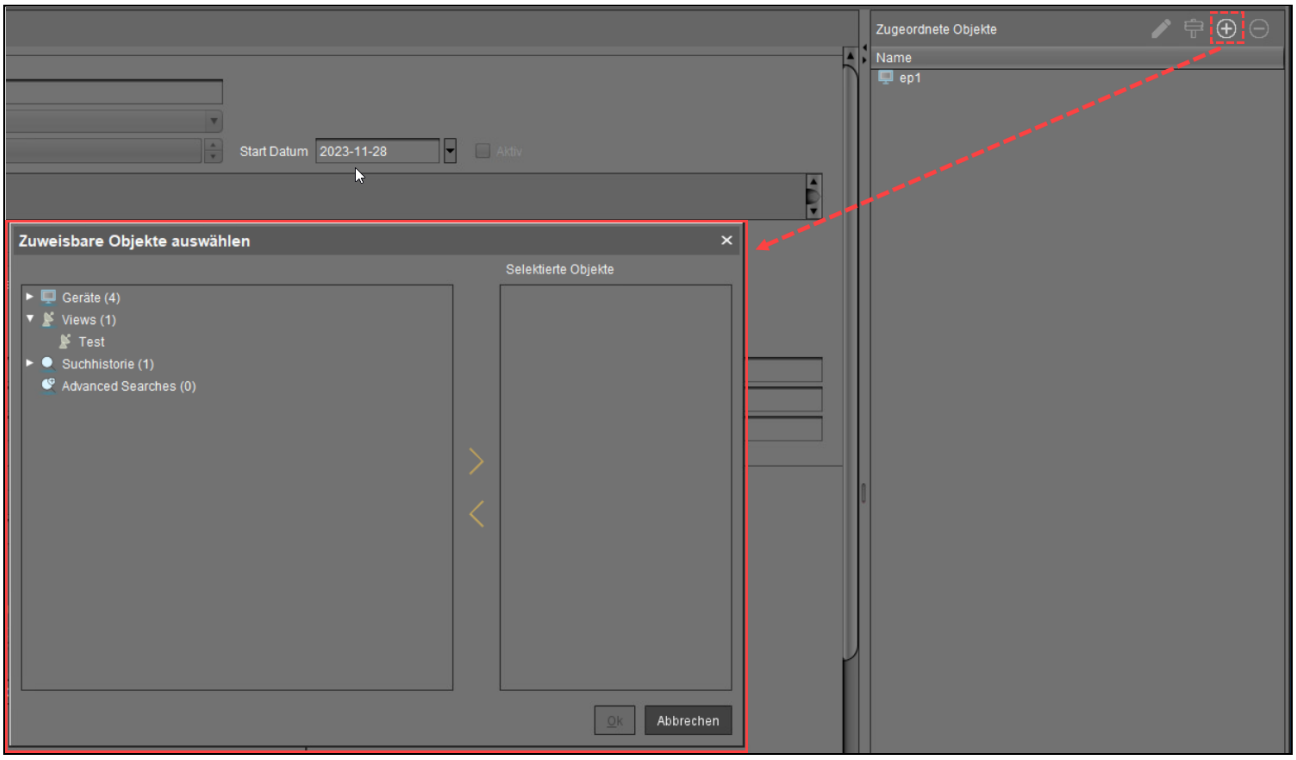
Auch die Geräte selbst erhaltenen einen Status für die Aufgabenausführung:

Läuft	Befehl wird gerade ausgeführt. Server wartet auf Antwort.
Wartet	Die Aufgabe läuft, der Befehl wird ausgeführt, wenn der nächste Prozess verfügbar ist.
Übertragen	Der Befehl wurde erfolgreich ausgeführt bzw. dem Gerät übertragen.

Abgebrochen	Aufgrund eines internen Fehlers oder einer unbekannten Ursache abgebrochen.
Fehlgeschlagen	Befehl konnte nicht ausgeführt werden, Grund wird in der Meldungsspalte angezeigt.
Beim nächsten Booten	Befehl wird beim nächsten Gerätestart ausgeführt.
Nicht bearbeitet	Befehl wurde nicht ausgeführt, weil das Time-out der Aufgabe erreicht wurde.

Zuordnung

Über die Objektzuweisung können Aufgaben den Geräten zugewiesen werden.



Über die **Hinzufügen (+)** können Sie die folgenden Zuweisungen verwenden:

- Sie können bestimmte Geräte auswählen.
- Sie können ein Geräteverzeichnis auswählen. Der Auftrag wird dann allen Geräten zugewiesen, die sich zum Zeitpunkt der Ausführung in diesem Verzeichnis befinden.
- Sie können die dynamische Geräteauswahl nutzen, indem Sie eine View / Suche / Advanced Search auswählen. Zum Ausführungszeitpunkt werden die Geräte zunächst anhand der Auswahlbedingungen der View / Suche / Advanced Search ermittelt. Anschließend werden ihnen die Aufträge zugewiesen.

Um eine statische Gerätezuweisung durch die MAC-Adresse oder eine dynamische Zuweisung über das Verzeichnis oder die View zu erstellen, ist eine Schreibberechtigung für die entsprechenden Objekte erforderlich. Zum Zeitpunkt der Ausführung muss der Benutzer, der die Aufgabe erstellt hat, über die Schreibberechtigung für das betreffende Gerät verfügen. Dies muss berücksichtigt werden, wenn auch

andere Benutzer eine Schreibberechtigung für eine Aufgabe haben, insbesondere wenn der Datenbankbenutzer eine Aufgabe erstellt hat.

Dateien - Dateien am IGEL UMS Server registrieren und zu Geräten übertragen

Mittels einer Funktion zur **Dateiübertragung** in der IGEL Universal Management Suite (UMS) können Sie Dateien im lokalen Dateisystem des Geräts speichern. Eine Datei muss auf dem UMS Server registriert werden, bevor sie an das Gerät gesendet werden kann. Beispiele sind lokal am Gerät benötigte Virenscannersignaturen, Browserzertifikate, Lizenzinformationen, usw. Informationen zur Dateiverwaltung in der IGEL UMS Web App finden Sie unter Upload and Assign Files in the IGEL UMS Web App (see page 855).

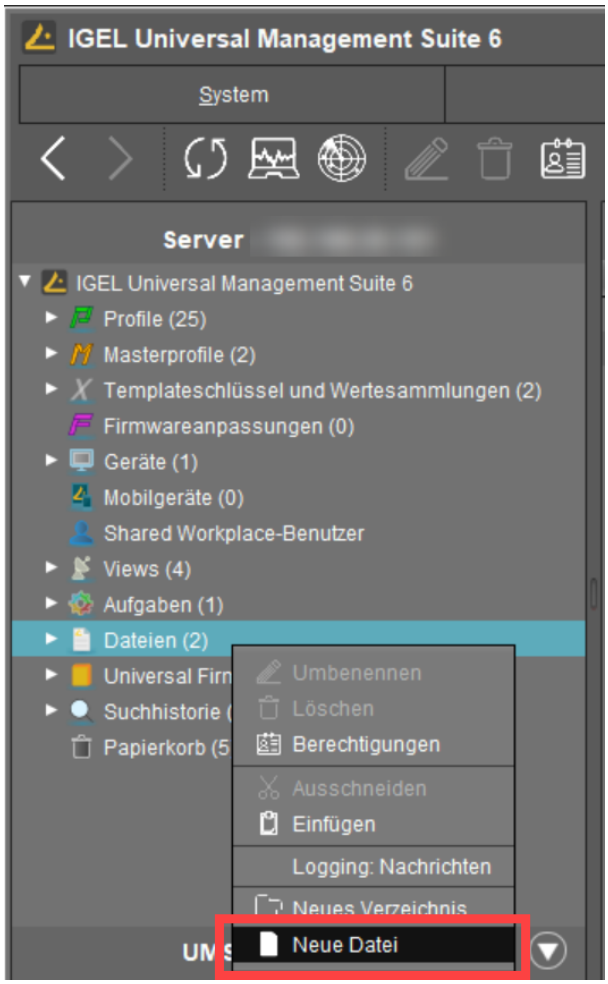
Menüpfad: **Dateien > [Kontextmenü] > Neue Datei**

Datei am UMS Server registrieren

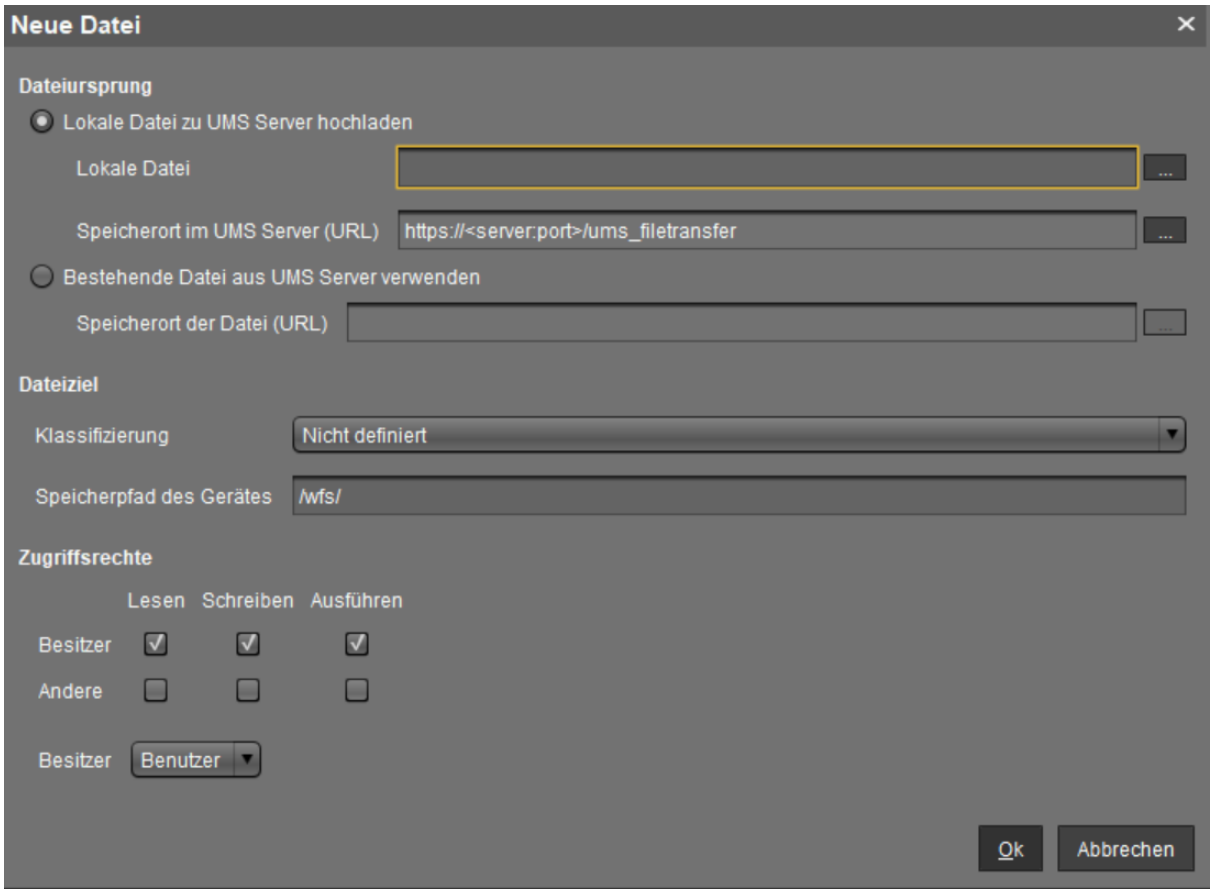
Um eine Datei auf ein Gerät zu laden, muss sie zunächst auf dem UMS Server registriert werden.

So registrieren Sie eine Datei auf dem UMS Server:

1. Wählen Sie in der UMS Konsole **Dateien > [Kontextmenü] > Neue Datei** oder **System > Neu > Neue Datei**.



2. Wählen Sie unter **Dateiursprung** eine lokale Datei oder eine bereits auf dem Server befindliche aus.



3. Wählen Sie den **Speicherort im UMS Server (URL)** aus. Sie können nur das Verzeichnis `ums_filetransfer` oder darin erstellte Unterverzeichnisse verwenden.

4. Wählen Sie unter **Klassifizierung** den Typ der Datei aus. Dies dient zum automatischen Festlegen von geeigneten Speicherorten und Dateiberechtigungen. Wählen Sie zwischen:
   - **Nicht definiert**
   - **Webbrowserzertifikat**
   - **SSL-Zertifikat**
   - **Java Zertifikat**
   - **IBM iAccess Zertifikat**
   - **App Signing Zertifikat**
   - **Allgemeines Zertifikat**

   Informationen zur Zertifikatsbereitstellung finden Sie unter Vertrauenswürdige Stammzertifikate in IGEL OS einspielen.

5. Bei Klassifizierung als **Nicht definiert** geben Sie unter **Speicherpfad des Gerätes** den Pfad auf dem lokalen Dateisystem des Geräts an.
   Wenn Sie ein Verzeichnis eingeben, das noch nicht existiert, wird dann dieses automatisch erstellt.

Beachten Sie, dass Pfade mit einem Pfadtrenner - Slash "/" oder Backslash "\" - enden müssen.

Aufgrund der begrenzten Speicherkapazität wird die Verwendung des Ordners `/wfs/` für große Dateien (>2 MB) NICHT empfohlen.

6. Bei Klassifizierung als **Nicht definiert** vergeben Sie **Zugriffsrechte** und den **Besitzer**.
   Diese werden der Datei bei der Übertragung an das Gerät mitgegeben und auf dem Zielsystem angewendet.

7. Bestätigen Sie die Einstellungen mit **OK**.
   Die Datei wird jetzt in die Webressource kopiert und auf dem UMS Server registriert.

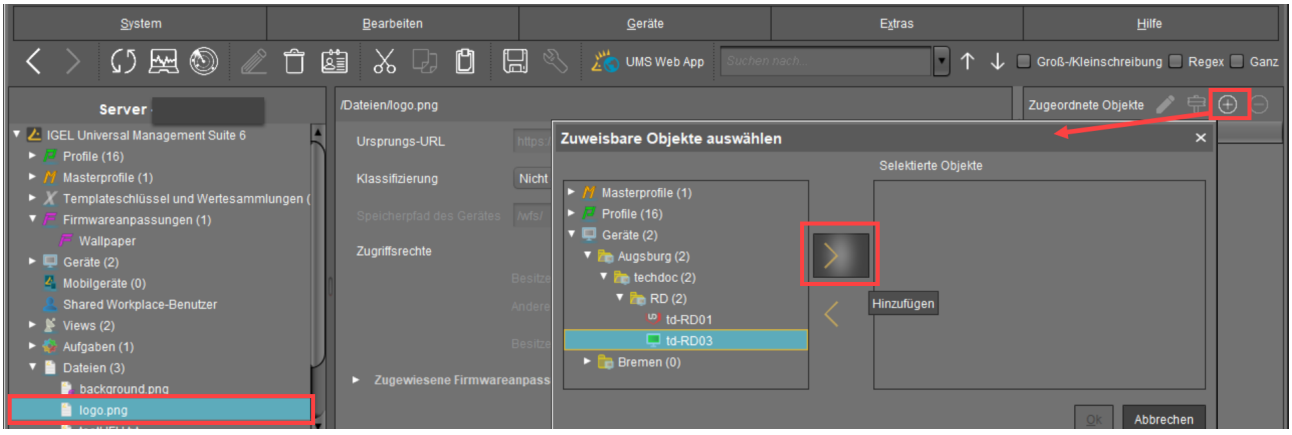
Registrierte Dateien werden automatisch zwischen den UMS Servern synchronisiert. Weitere Informationen finden Sie unter Welche Dateien werden automatisch zwischen den IGEL UMS Servern synchronisiert? (see page 151)

Datei zum Gerät übertragen

Um eine registrierte Datei auf ein Gerät hochzuladen, muss sie einem Gerät entweder direkt oder indirekt über ein Geräteverzeichnis oder ein Profil zugewiesen werden. Ist eine Datei einem Profil zugewiesen, wird sie dann mit den Profileinstellungen an die Geräte übertragen, wenn Sie dieses Profil den Geräten zuweisen.

▶ Ziehen Sie die Datei per Drag-and-Drop auf das Gerät / Geräteverzeichnis oder auf das Profil. Alternativ klicken Sie das Symbol ⊕ im Bereich **Zugeordnete Objekte**; Sie können den Bereich **Zugeordnete Objekte** in den Baumknoten **Dateien**, **Geräte** oder **Profile** verwenden.

Beispiel:

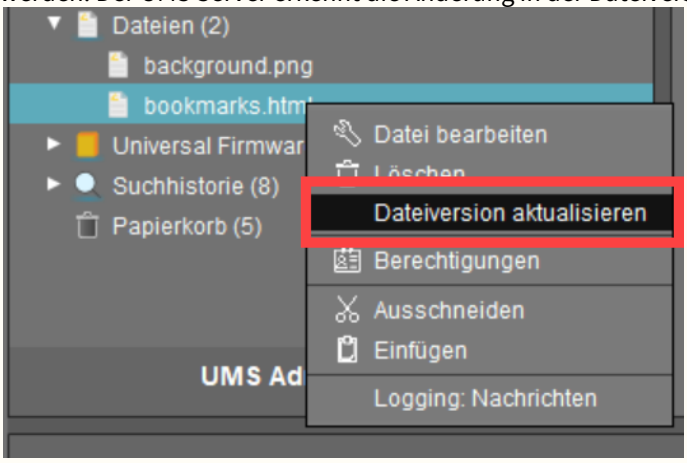


Eine so zugewiesene Datei wird beim Übertragen der UMS Einstellungen auf das Gerät kopiert, z. B. während das Gerät hochfährt. Solange die Datei dem Gerät zugewiesen ist, wird sie mit der auf dem UMS Server registrierten

Datei synchronisiert, wenn z. B. die Datei `bookmarks.html` durch eine neue Version ersetzt wird. Die MD5-Prüfsumme der dem Gerät zugewiesenen Datei wird mit der registrierten Datei verglichen. Wenn die Prüfsummen voneinander abweichen, wird die Datei erneut übertragen.

Dateiversion aktualisieren

Wenn eine Datei direkt im Dateisystem im Verzeichnis `ums_filetransfer` ersetzt wurde, muss sie in der UMS Konsole mit dem Befehl **Dateiversion aktualisieren** aus dem Kontextmenü der Datei aktualisiert werden. Der UMS Server erkennt die Änderung in der Dateiversion sonst nicht.



Danach klicken Sie im Kontextmenü des Gerätes oder unter **Geräte** in der Menüleiste auf **Weitere Befehle > Einstellungen UMS->Gerät**, um die Übertragung der Einstellungen an die Geräte zu beschleunigen.

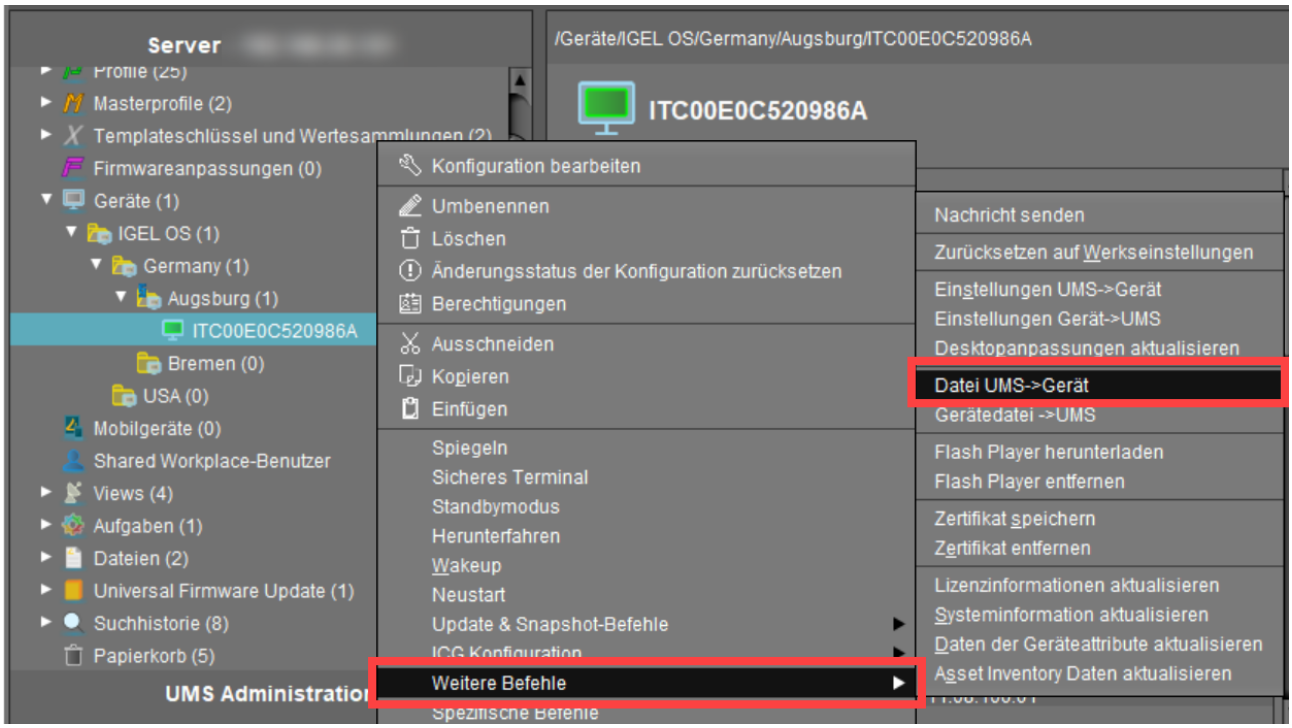
Ab UMS Version 5.02.100 kommt bei der Dateiübertragung die IP-Adresse der UMS zum Einsatz, so dass die Übertragung auch bei DNS-Problemen funktioniert.

Übertragung einer Datei ohne Zuweisung

Eine auf dem UMS Server registrierte Datei kann auch ohne Zuweisung auf das Gerät übertragen werden:

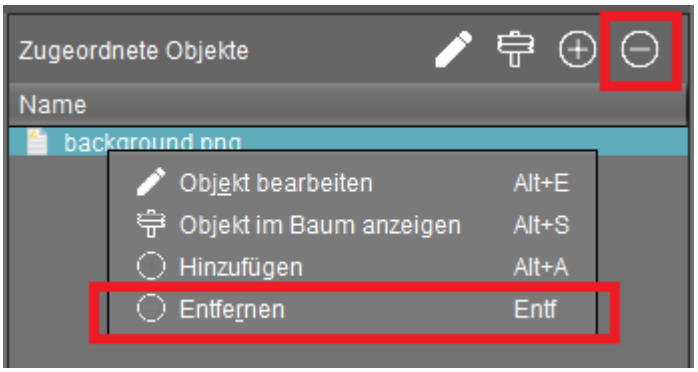
▶ Wählen Sie **Weitere Befehle > Datei UMS->Gerät** aus dem Kontextmenü des Geräts oder unter **Geräte** in der Menüleiste.

Dies ist ein einfacher Dateikopiervorgang. Es erfolgt KEINE Dateiaktualisierung, wenn sich die Dateiversion auf dem UMS Server ändert.

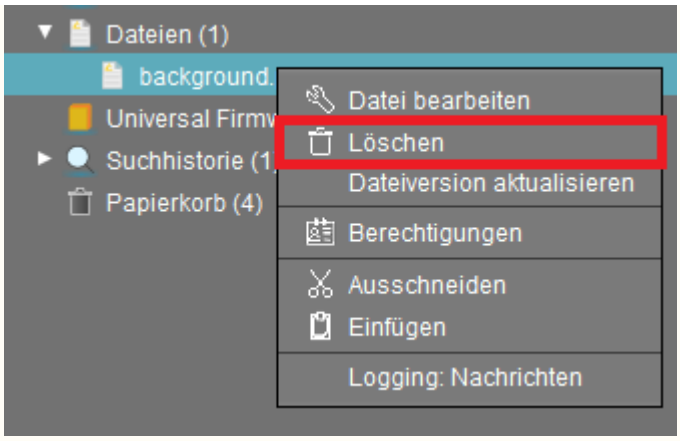


Datei vom Gerät entfernen

▶ Um eine Datei permanent vom Gerät zu löschen, wählen Sie das Gerät im Strukturbaum aus und entfernen Sie die Dateizuweisung im Bereich **Zugeordnete Objekte**.



⚠ Wenn Sie eine Datei im Strukturbaum unter **Dateien** löschen, wird sie von ALLEN Geräten entfernt, denen sie zugewiesen wurde.



IGEL Tech Video

Siehe auch IGEL Community Tech Video zur Übertragung von Dateien zu IGEL OS:

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=7EFCiZvlNPM

Datei auf den IGEL UMS Server übertragen

Der folgende Artikel erklärt, wie Sie eine Datei von Ihrem Endgerät auf die IGEL Universal Management Suite (UMS) übertragen können.

So laden Sie eine auf dem Gerät vorhandene Datei in die Webressourcen herunter:

▶ Klicken Sie im Kontextmenü eines Geräts oder unter **Geräte** in der Menüleiste auf **Weitere Befehle > Gerätedatei->UMS**.

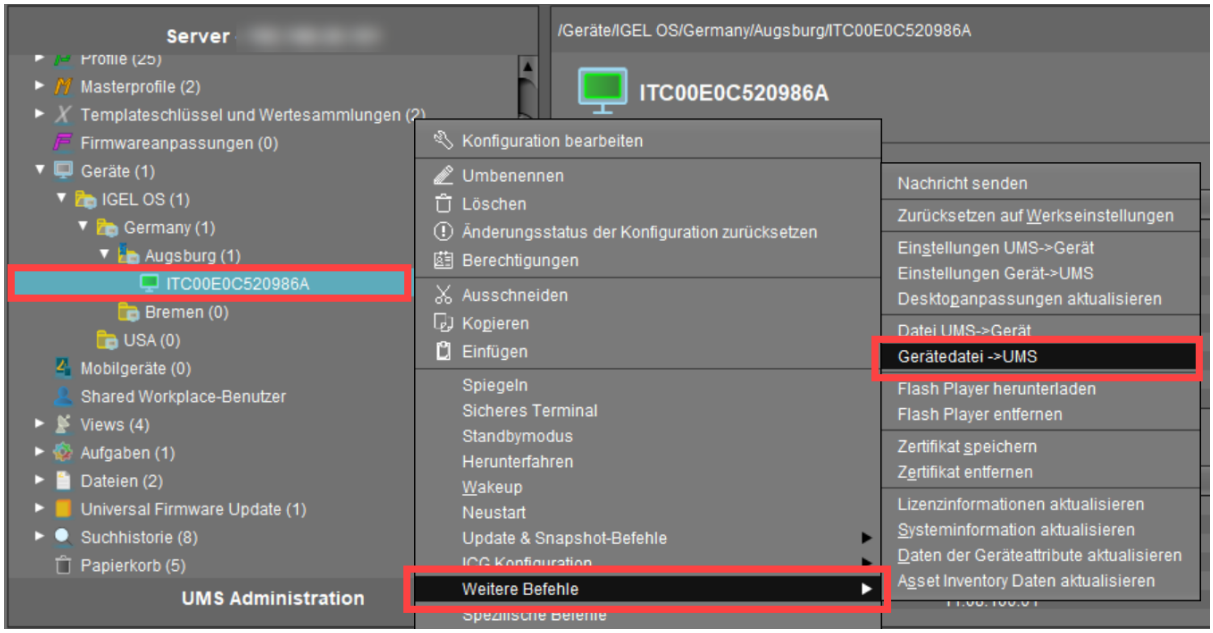
Die UMS kann das lokale Dateisystem des Geräts nicht durchsuchen. Sie müssen den Speicherort und den Namen der Datei kennen, die Sie in die Webressource laden möchten.

> ⓘ Eine vom Gerät zu WebDAV übertragene Datei wird nicht automatisch auf dem UMS Server registriert, sie befindet sich dann im Bereich des http-Servers der UMS. Sie können vorhandene Dateien aber nachträglich über **Dateien > Neue Datei** registrieren, siehe Dateien - Dateien am IGEL UMS Server registrieren und zu Geräten übertragen (see page 529).

Beispiel für die Verwendung des Befehls "Gerätedatei->UMS"

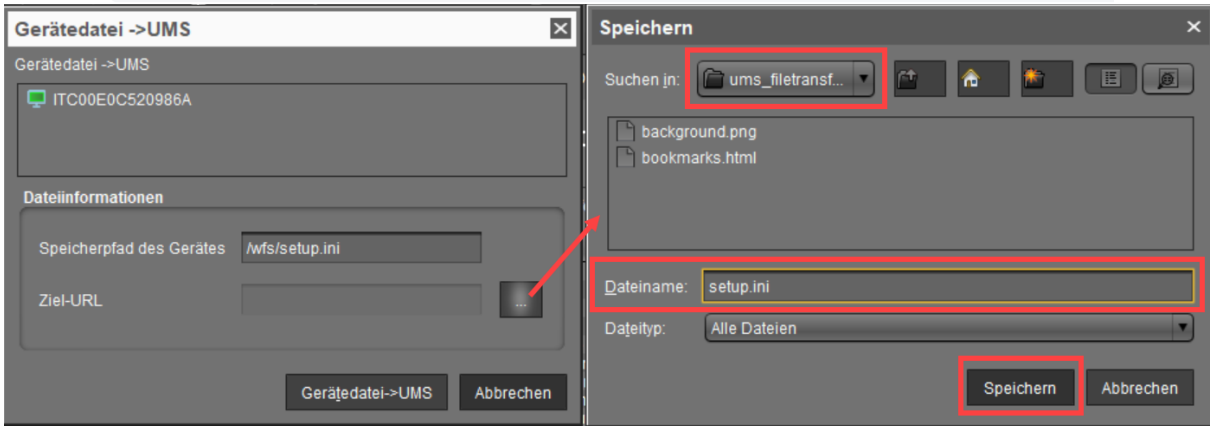
Der Befehl **Gerätedatei->UMS** kann verwendet werden, wenn Sie zum Beispiel die aktuelle lokale Konfiguration des Geräts auslesen und daher die beiden lokalen Dateien `setup.ini` und `group.ini` über die UMS kopieren müssen:

1. Wählen Sie in der UMS Konsole aus dem Kontextmenü des Geräts **Weitere Befehle > Gerätedatei->UMS**.

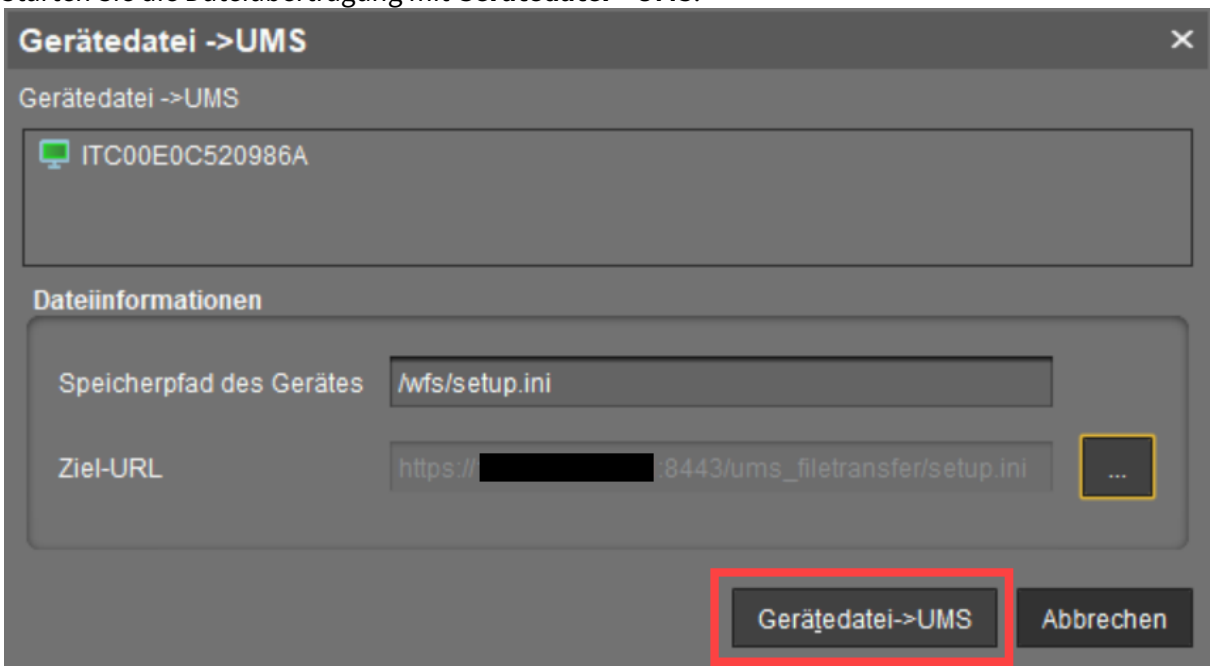


2. Geben Sie unter **Speicherpfad des Gerätes** als Quelle `/wfs/` an.
   Beispiel: `/wfs/setup.ini`

3. Wählen Sie unter **Ziel-URL** das Ziel auf dem UMS Server aus und geben Sie unter **Dateiname** den Namen der übertragenen Datei ein.
   Beispiel: `https://umsserver.domain:8443/ums_filetransfer/setup.ini`



4. Starten Sie die Dateiübertragung mit **Gerätedatei->UMS**.



Weitere Informationen zum Auslesen der lokalen Gerätekonfiguration finden Sie auch unter Lokale Konfiguration des IGEL OS Geräts exportieren.

Updating File Version in IGEL UMS

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

Universal Firmware Update

Menüpfad: **Server - [Adresse des UMS Servers] > Universal Firmware Update**

In diesem Bereich können Sie nach neuen Firmwareupdates für IGEL Geräte und für mit OSC konvertierte Geräte suchen, die Konfigurationsdaten für bestimmte Firmwareversionen importieren und die Firmwaredateien zur Verteilung bereitstellen.

Im Kontextmenü stehen folgende Optionen zur Verfügung:

- Neue Universal Firmware Updates suchen (see page 540)
- **Snapshot -> Universal Firmware Update**
- **Firmware archive (Zip-Datei) -> Universal Firmware Update**
- **Berechtigungen**. Siehe Zugriffsrechte (see page 678).

Wenn Sie **Snapshot -> Universal Firmware Update** oder **Firmware archive (Zip-Datei) -> Universal Firmware Update** auswählen, können Sie eine der folgenden Optionen auswählen:

- Firmwares exportieren (see page 468): Importiert die Konfigurationsdaten für bestimmte Firmwareversionen aus XML-Dateien, die von einer UMS Instanz erzeugt wurden.
- Snapshot -> Universal Firmware Update (see page 541): Registriert einen Windows Embedded Standard Snapshot als Universal Firmware Update.
- Firmwarearchiv (Zip-Datei) -> Universal Firmware Update (see page 542): Registriert die Firmwaredateien für IGEL OS als Universal Firmware Update.

⚠ Wenn Sie die Updatedateien bereitgestellt haben, müssen Sie sie den Geräten zuweisen und den Updateprozess starten. Siehe dazu Updates zuweisen (see page 463).

ⓘ Sie können einen FTP-Server verwenden, um Firmwareupdates auf Geräte zu verteilen, als Alternative zur WebDAV-Funktionalität der UMS. Wenn Ihre Geräte über ICG verbunden sind, ist ein FTP-Server erforderlich. Weitere Informationen finden Sie unter Universal Firmware Update (1) (see page 539).
Wenn Sie eine High-Availability-Umgebung haben und WebDAV zum Herunterladen der Firmwareupdates verwenden, lesen Sie Welche Dateien werden automatisch zwischen den IGEL UMS Servern synchronisiert? (see page 151).

IGEL Tech Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=XflN_BEyDZc

Neue Universal Firmware Updates suchen

Menüpfad: **Server - [Adresse des UMS Servers] > Universal Firmware Update >** [Kontextmenü] **> Neue Universal Firmware Updates suchen**

In diesem Bereich können Sie den öffentlichen IGEL Server nach Firmwareupdates durchsuchen, die von der UMS heruntergeladen und als Universal Firmware Updates zur Verfügung gestellt werden.

Die Symbole oben rechts im Fenster haben folgende Bedeutung:

	Ein WebDAV-Verzeichnis als Zielverzeichnis auswählen
	FTP-Zielverzeichnis festlegen
	Änderung rückgängig machen

Universal Firmware Updates

Aufnehmen

☑ Die entsprechende Firmware wird heruntergeladen.

Modell: Name der Firmware.

Version: Versionsnummer der Firmware zum Auswählen.

Zielverzeichnis: Verzeichnis, in das die Firmware geladen wird.
Das ist der `ums_filetransfer` Ordner oder beim FTP-Server das Verzeichnis, das unter **UMS Administration > Globale Konfiguration > Universal Firmware Update** festgelegt wurde.

Release Notes: Zur entsprechenden Firmware gehörige Release Notes als HTML-Seite oder im Textformat.

Zeige nur neue Firmware-Versionen (blendet bereits heruntergeladene Versionen aus)

☑ Nur die aktuellste Version der jeweiligen Modelle wird angezeigt. Ist die aktuellste Version schon in die UMS heruntergeladen, wird sie nicht mehr angezeigt.

☐ Alle verfügbaren Versionen werden angezeigt. (Standard)

Herunterladen: Das Update wird zum UMS Strukturbaum hinzugefügt, und der aktuelle Verarbeitungsstatus wird angezeigt.

Snapshot -> Universal Firmware Update

Menüpfad: **Server - [Adresse des UMS Servers] > Universal Firmware Update >** [Kontextmenü] **> Snapshot -> Universal Firmware Update**

In diesem Bereich können Sie einen Snapshot eines Geräts mit Windows Embedded Standard als Universal Firmware Update registrieren. Der Snapshot wird in einem WebDAV-Verzeichnis abgelegt.

Snapshot-Datei: Name der Snapshotdatei.

Snapshot auswählen: Öffnet einen Dialog zur Auswahl der Snapshotdatei. Es können nur Snapshotdateien mit einer SNP-Dateiendung hochgeladen werden.

Name: Name des angepassten Snapshots.

Firmwarearchiv (Zip-Datei) -> Universal Firmware Update

Menüpfad: **Server - [Adresse des UMS Servers] > Universal Firmware Update >** [Kontextmenü] **> Firmwarearchiv (Zip-Datei) -> Universal Firmware Update**

In diesem Bereich können Sie Updates von einer lokalen Quelle laden. Die Firmwareateien werden in einem WebDAV-Verzeichnis abgelegt.

> Eine Firmware von einer lokalen Quelle besitzt nicht die Metainformationen, die auf dem IGEL Server hinterlegt sind.

Firmwaredatei: Pfad und Name der zip-Datei. Beispiel: `c:\Updates\IGEL_LINUX_10.03.100.zip`, mit Dateiauswahl wählbar

Displayname: Namen für die Anzeige des Updates in der UMS.

WebDAV-Zielverzeichnis: Verzeichnis, in das das Update gespeichert wird, um es an die Geräte zu verteilen.

Suchhistorie

Menüpfad: **Strukturbaum > Suchhistorie**

Hier werden alle Suchanfragen als eigene Objekte gespeichert und können über das Kontextmenü weiter bearbeitet werden.

Mögliche Suchtypen:

- Geräte
- Profile
- Views

- Kontextmenü einer Suchanfrage (see page 544)

Kontextmenü einer Suchanfrage

Menüpfad: **Strukturbaum > Suchhistorie**

Folgende Optionen stehen Ihnen im Kontextmenü einer Suchanfrage zur Verfügung:

- **Löschen**: Löscht das Suchergebnis aus der Liste.
- **Suche bearbeiten**: Ermöglicht eine Änderung der Suchanfrage. Die Bearbeitung der Suche ist nur im Expertenmodus möglich. Details zum Expertenmodus finden Sie unter Expertenmodus (see page 492). Der Text-Expertenmodus ist nur für den Suchtyp **Geräte** möglich.

Die folgenden Optionen sind immer dann aktiv, wenn **Automatisch Anzahl und Objekte laden** unter **Menüleiste > Extras > Einstellungen > Views und Suchen > Seitenverhalten > Wenn ein Suchergebnis geladen wird...** ausgewählt wird. Wird dort einer der anderen Parameter ausgewählt, sind die folgenden Optionen erst dann aktiv, wenn eine Schaltfläche **Gerät laden** (oder **Profil laden** / **View laden**) im Inhaltsbereich der Suchanfrage angeklickt wird.

- **Speichern unter...**: Speichert das Suchergebnis in einem der folgenden Dateiformate: XSL-FO, CSV, HTML oder XML.

Folgende Optionen sind nur dann aktiv, wenn Sie **Geräte** als Suchtyp gewählt haben:

- **Objekte zu den Geräten der Suche zuordnen...**: Ordnet den gesuchten Geräten Objekte zu. Zur Vorgehensweise siehe Einer View Objekte zuordnen (see page 517).
- **Objekte von den Geräten der Suche entfernen...**: Entfernt die zugeordneten Objekte.

Papierkorb - Löschen von Objekten in der IGEL UMS

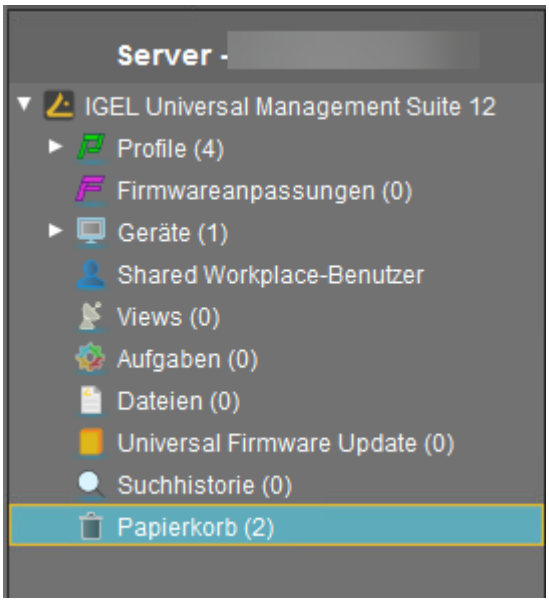
In der IGEL Universal Management Suite (UMS) haben Sie die Möglichkeit, Objekte im **Papierkorb** abzulegen. Wenn der Papierkorb deaktiviert ist, werden die Objekte sofort dauerhaft gelöscht.

Der Papierkorb wird global für alle Benutzer der UMS aktiviert oder deaktiviert.

> Sie können den Papierkorb unter **UMS Konsole > UMS Administration > Globale Konfiguration > UMS Features** aktivieren / deaktivieren.

> Wenn Sie Ihr Endgerät nicht in der UMS registrieren können, wird empfohlen zu prüfen, ob sich das Gerät im Papierkorb befindet. Wenn ja, stellen Sie das Gerät aus dem Papierkorb wieder her oder löschen Sie es aus dem Papierkorb und registrieren Sie es erneut.
> Für weitere Lösungen, siehe Troubleshooting: Die Registrierung eines Geräts über Suche nach Geräten schlägt fehl (see page 165).

Menüpfad: **UMS Konsole > Papierkorb**



Wird nun ein Objekt im Strukturbaum gelöscht (Funktion **Löschen** in der Symbolleiste, im Kontextmenü oder Taste [Entf]), so wird es nach Bestätigung in den **Papierkorb** verschoben.

> Bei aktivem Papierkorb lassen sich Objekte auch direkt und endgültig löschen mit [Umschalt-Entf].

Verzeichnisse werden mitsamt ihrer Unterordner und aller Elemente in den Papierkorb verschoben und können so als komplette Struktur auch wiederhergestellt werden. Elemente im Papierkorb lassen sich dort endgültig löschen oder auch wiederherstellen – rufen Sie dazu das Kontextmenü eines Elements im Papierkorb auf.

> Sollte sich das Kontextmenü für Elemente im **Papierkorb** nicht aufrufen lassen, so ist der Papierkorb wahrscheinlich inaktiv. Prüfen Sie den Status des Papierkorbs wie oben beschrieben.

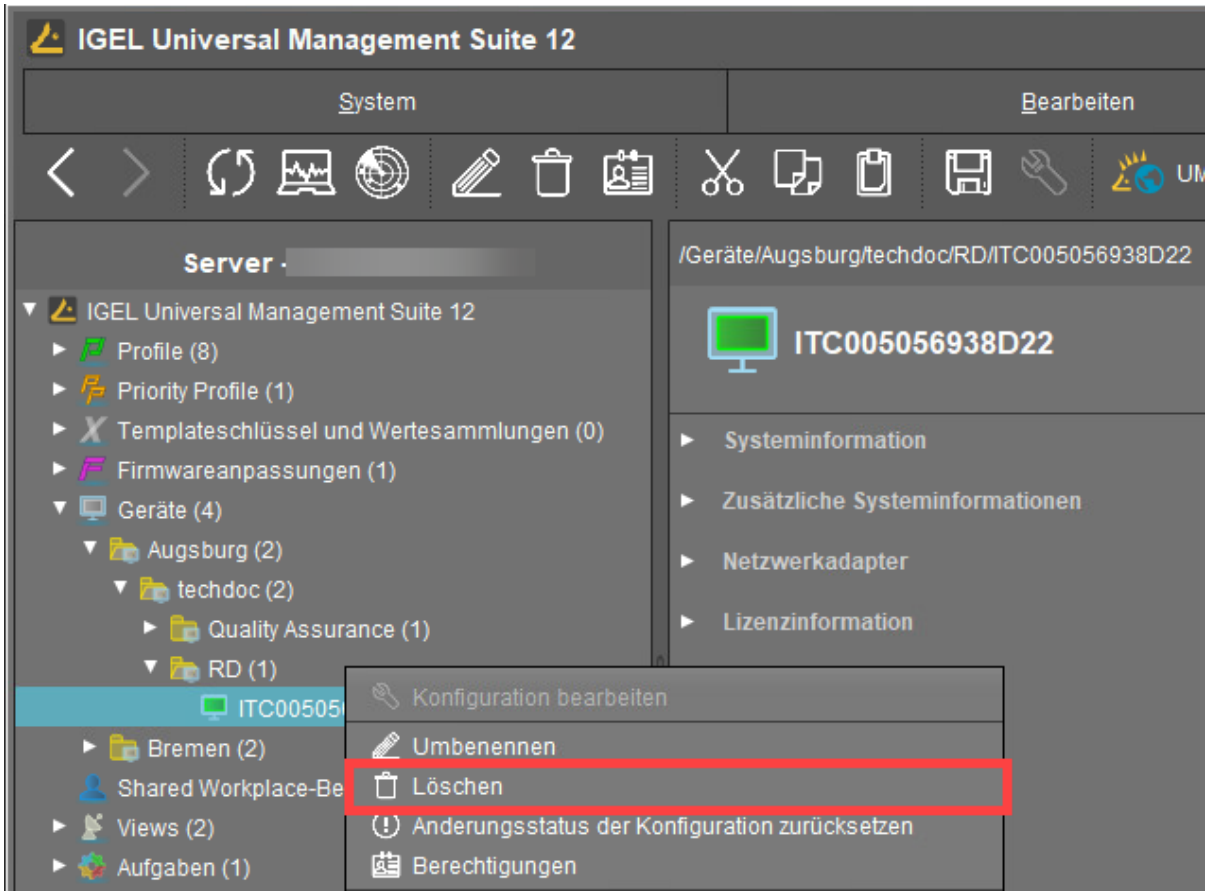
Es lassen sich fast alle Elemente aus dem UMS Strukturbaum in den Papierkorb verschieben: Geräte, Profile, Views, Aufgaben, Dateien und deren Verzeichnisse. Nicht löschen lassen sich Shared Workplace-Benutzer. Nur endgültig löschen lassen sich Administratorkonten (in der Kontenverwaltung). Elemente der Suchhistorie können auch nur endgültig gelöscht werden (mit [Umschalt-Entf] oder mit Funktion **Löschen** im Kontextmenü). Ebenfalls nicht gelöscht werden können die jeweils obersten Knoten im Strukturbaum – allerdings wirkt sich dieser Vorgang auf alle löschbaren Elemente unterhalb dieses Knotens aus!

- Objekte im Papierkorb werden weder von der Suchfunktion noch durch Views gefunden und lassen sich auch nicht durch geplante Aufgaben ansprechen.
- Geräte im Papierkorb erhalten keine neuen Einstellungen von der UMS mehr, bleiben aber an der UMS registriert und können aus dem Papierkorb mit allen Profilzuordnungen wiederhergestellt werden.
- Profile im Papierkorb sind nicht mehr wirksam, es ändern sich ggf. also Einstellungen von Geräten. Die Wiederherstellung von Profilen lässt auch deren Zuordnungen zu Geräten wieder aktiv werden.
- Geplante Aufgaben, Views und Suchanfragen im Papierkorb werden nicht ausgeführt.
- Zuordnungen von Profilen, Dateien, Views und Firmware Updates im Papierkorb sind nicht aktiv.

Geräte aus der UMS entfernen

So löschen Sie Geräte in der UMS:

1. Gehen Sie in der UMS Konsole unter **Geräte > [Kontextmenü des Geräts]** und klicken Sie **Löschen**.



2. Nur für IGEL OS 12-Geräte: Bestimmen Sie im Dialog **Löschen bestätigen**, ob die Lizenzen gelöscht werden sollen, und akzeptieren Sie die **Geschäftsbedingungen**.
   Wenn Sie **Lizenzen löschen** aktivieren:
   - werden alle Lizenzen von dem Gerät entfernt, wenn das Gerät online ist (Geräteebene)
   - werden alle Lizenzen, die in der UMS für das Gerät registriert sind, von der UMS entfernt (UMS-Ebene)
   - aus allen registrierten Product Packs werden die entsprechenden Unit IDs entfernt, wenn das IGEL Lizenz-Portal (ILP) erreicht werden kann (ILP-Ebene)

     Damit sind die betroffenen Lizenzen vollständig entfernt und können für ein anderes Gerät verwendet werden.

Wenn der Papierkorb aktiviert ist, wird der Dialog **Löschen bestätigen** angezeigt, wenn die Geräte aus dem Papierkorb gelöscht werden.

UMS Administration

UMS Netzwerk

Menüpfad: **UMS Administration > UMS Netzwerk**

Hier können Sie UMS Server, UMS Load Balancer und IGEL Cloud Gateways (ICG) ansehen und verwalten.

- Server - Informationen zu Ihrem UMS Server anzeigen (see page 551)
- Load Balancer - Informationen zu Ihrem IGEL UMS Load Balancer anzeigen (see page 554)
- IGEL Cloud Gateway (see page 556)

Server - Informationen zu Ihrem UMS Server anzeigen

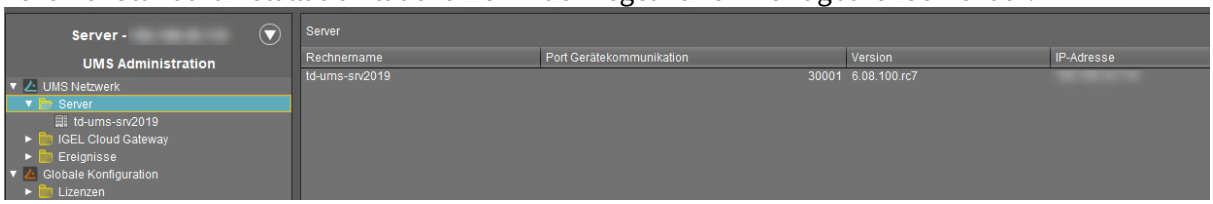
Im **Server**-Knoten der IGEL Universal Management Suite (UMS) Konsole finden Sie grundlegende Informationen zu allen Servern, die zu Ihrer UMS Installation gehören. Für einen einzelnen Server sind zusätzliche Details wie Prozessinformationen, Dienststatus, statistische Daten usw. verfügbar. Sie können hier auch die Öffentliche Adresse und den Öffentlichen Web-Port für Ihren UMS Server festlegen.

Menüpfad: **UMS Konsole > UMS Administration > UMS Netzwerk > Server**

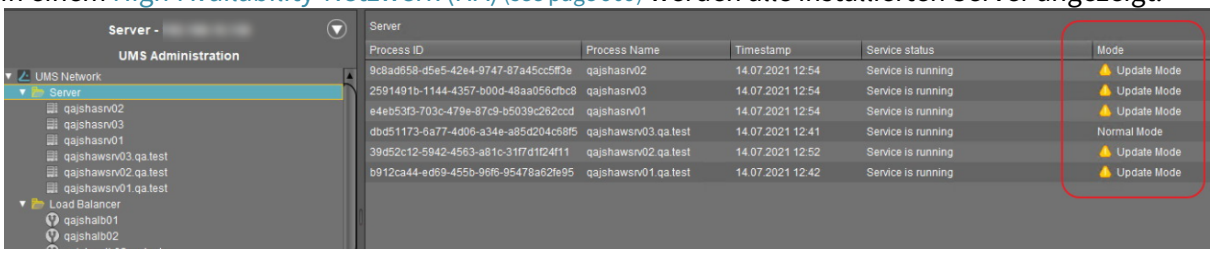
"Server"-Knoten in der IGEL UMS

Der Knoten **Server** listet alle zur UMS Installation gehörenden Server:

- Bei einer Standardinstallation taucht hier in der Regel nur ein verfügbarer Server auf.



- In einem High-Availability-Netzwerk (HA) (see page 909) werden alle installierten Server angezeigt.



> **Normaler Modus und Updatemodus (nur für HA-Installationen)**
> Ein Server befindet sich immer dann im normalen Modus, wenn er sich nicht temporär während einer UMS HA-Aktualisierung mit der eingebetteten Update-Datenbank verbunden hat, siehe HA-Installation aktualisieren: Ohne Ausfallzeit der Server (see page 938). **Normaler Modus** bedeutet also, dass der Server mit der normalen "Run-Konfiguration" läuft, und nicht mit einer Datenbank, die sich im Updatemodus befindet.

Einzelner Server

Für einen einzelnen Server sind die folgenden grundlegenden Optionen verfügbar.

Statusanzeigen für den UMS Server

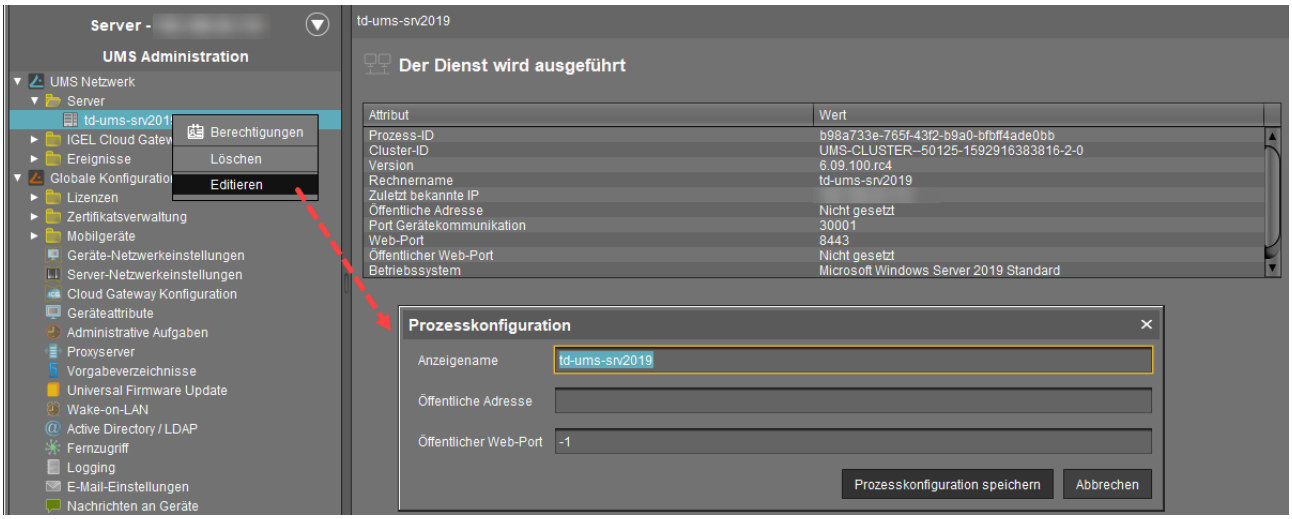
Der Status der Server wird durch die folgenden Symbole angezeigt:

	Der Server ist online.
	Der Server ist offline.
	Der Status des Servers ist unbekannt (z. B. wenn ein neuer Server im Netzwerk propagiert wird).

Prozesskonfiguration für den IGEL UMS Server

Für jeden Server können Sie die Prozesskonfiguration bearbeiten, z. B. Sie können den **Anzeigenamen** für den UMS Server ändern. Sie können hier auch die **Öffentliche Adresse** und den **Öffentlichen Web-Port** konfigurieren.

▶ Um die Prozesskonfiguration zu bearbeiten, klicken Sie im Kontextmenü des entsprechenden Servers auf **Editieren**.



Falls festgelegt, werden **Öffentliche Adresse** und **Öffentlicher Web-Port** für Folgendes verwendet:

- beim Zugriff auf Dateien, die in der UMS Konsole unter **Dateien** erstellt wurden (siehe Dateien - Dateien am IGEL UMS Server registrieren und zu Geräten übertragen (see page 529)), und auf Universal Firmware Updates (siehe Universal Firmware Update (see page 539))
- für interne Kommunikation zwischen den UMS Servern (inkl. Dateisynchronisation zwischen den UMS Servern; siehe Welche Dateien werden automatisch zwischen den IGEL UMS Servern synchronisiert? (see page 151), inkl. den Abschnitt "Während der Aktualisierung verwendete Verbindungsdaten")
- für die automatisch generierten Webzertifikate, siehe Web (see page 576)
- für HTTPS-Anfragen von Geräten, wenn keine Cluster-Adresse festgelegt wurde (siehe Server-Netzwerkeinstellungen in der IGEL UMS (see page 581))

ⓘ Als **Öffentliche Adresse** können Sie die IP-Adresse oder den FQDN des UMS Servers angeben. Die maximale Länge der **Öffentlichen Adresse** ist auf 255 Zeichen begrenzt.

Prozessaufgaben (nur für HA Installationen)

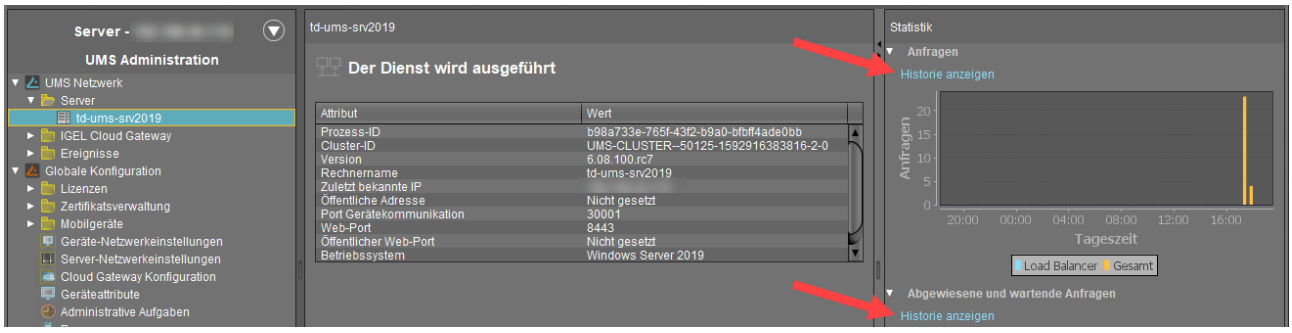
Im Falle der UMS HA-Installation können Sie auch den Dienst `IGEL RMGUIServer` starten, anhalten oder neu starten:

Wie Sie Dienste starten oder stoppen können, erfahren Sie auch unter IGEL UMS HA-Dienste und -Prozesse (see page 949).

Statistik für den UMS Server

Eine Übersicht der **Anfragen** und der **Abgewiesenen und wartenden Anfragen** durch Geräte erlaubt eine Einschätzung der Serverlast, wie sie sich über den betrachteten Zeitraum verteilt.

▶ Klicken Sie **Historie anzeigen**, um eine skalierbare Ansicht zu öffnen. Sie können mit der Maus in Ausschnitte hereinzoomen oder mittels Mausgeste (nach links ziehen mit gedrückter Maustaste) die Ansicht wiederherstellen.



Load Balancer - Informationen zu Ihrem IGEL UMS Load Balancer anzeigen

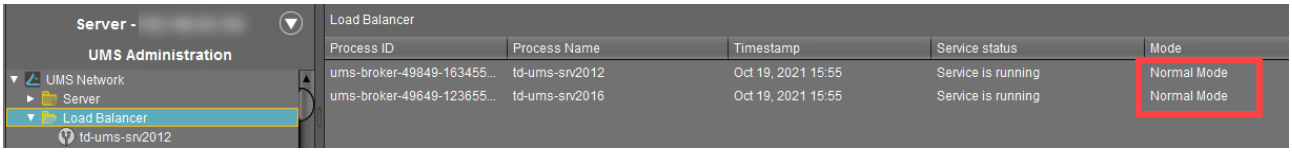
Im **Load Balancer**-Knoten der IGEL Universal Management Suite (UMS) Konsole finden Sie grundlegende Informationen zu allen Load Balancern, die zu Ihrer UMS Installation gehören. Für einen einzelnen Load Balancer sind zusätzliche Details wie Prozessinformationen, Dienststatus, statistische Daten usw. verfügbar.

Menüpfad: **UMS Administration > UMS Netzwerk > Load Balancer**

"Load Balancer"-Knoten in der IGEL UMS

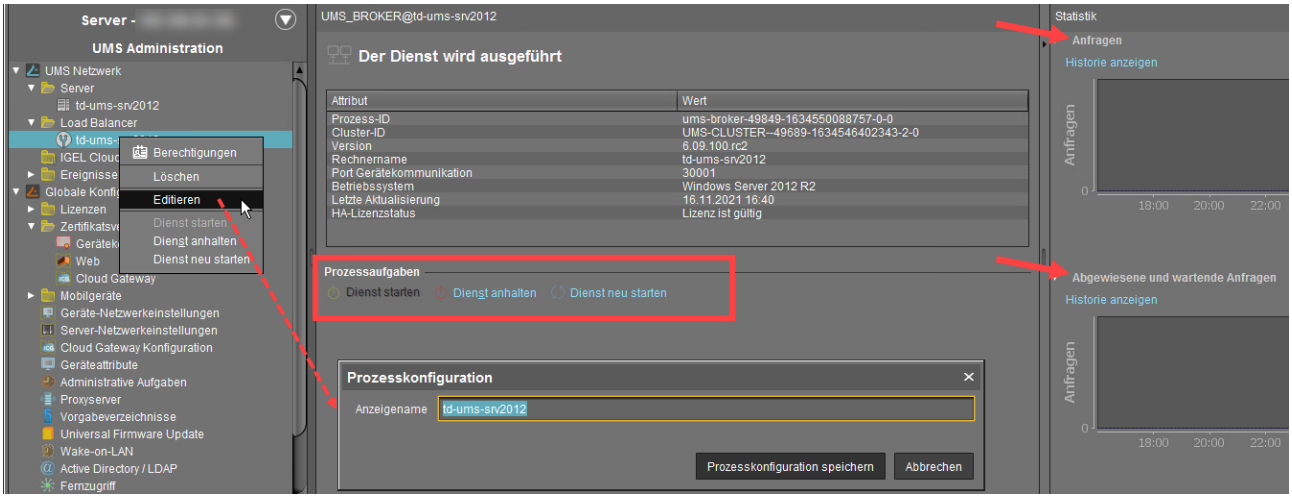
Der Knoten **Load Balancer** ist im UMS Strukturbaum nur dann sichtbar und aktiv, wenn Sie ein UMS High-Availability-Netzwerk mit **UMS Load Balancer** installiert haben. Siehe High Availability (HA) (see page 909).

Der Knoten **Load Balancer** listet alle zur UMS Installation gehörenden Load Balancer:



Normaler Modus bedeutet, dass der Load Balancer mit der normalen "Run-Konfiguration" läuft. Beachten Sie, dass dies nicht als Indikator für das allgemeine ordnungsgemäße Funktionieren von Load Balancern dient. Wenn Sie Ihre HA-Umgebung überprüfen möchten, siehe UMS HA Statusprüfung - Ihre High Availability- und Distributed UMS-Systeme analysieren (see page 944).

Einzelner Load Balancer



Statusanzeigen für den UMS Load Balancer

Der Status der Load Balancer wird durch die folgenden Symbole angezeigt:

	Der Load Balancer ist online.
	Der Load Balancer ist offline.
	Der Status vom Load Balancer ist unbekannt (z. B. wenn ein neuer Load Balancer im Netzwerk propagiert wird).

Prozesskonfiguration für den UMS Load Balancer

Für jeden Load Balancer können Sie die Prozesskonfiguration bearbeiten, z. B. Sie können den **Anzeigenamen** für den Load Balancer ändern.

▶ Um die Prozesskonfiguration zu bearbeiten, klicken Sie im Kontextmenü des entsprechenden Load Balancers auf **Editieren**.

Prozessaufgaben für den UMS Load Balancer

Unter **Prozessaufgaben** können Sie auch den `IGEL UMS Load Balancer`-Dienst starten, stoppen oder neu starten. Wie Sie Dienste starten oder stoppen können, erfahren Sie auch unter IGEL UMS HA-Dienste und -Prozesse (see page 949).

Statistik für den UMS Load Balancer

Eine Übersicht der **Anfragen** und der **Abgewiesenen und wartenden Anfragen** durch Geräte erlaubt eine Einschätzung der Serverlast, wie sie sich über den betrachteten Zeitraum verteilt.

▶ Klicken Sie **Historie anzeigen**, um eine skalierbare Ansicht zu öffnen. Sie können mit der Maus in Ausschnitte hereinzoomen oder mittels Mausgeste (nach links ziehen mit gedrückter Maustaste) die Ansicht wiederherstellen.

IGEL Cloud Gateway

Menüpfad: **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway**

Sie können die UMS hier mit einem oder mehreren IGEL Cloud Gateways (ICG) verbinden.

	Neues IGEL Cloud Gateway mit dem ICG Remote Installer installieren Siehe IGEL Cloud Gateway installieren.
	Das ausgewählte IGEL Cloud Gateway mit dem ICG Remote Installer deinstallieren. Wenn der IGEL Cloud Gateway mit dieser Funktion deinstalliert wurde, kann er mit dem ICG Remote Installer erneut installiert werden.
	Das ausgewählte IGEL Cloud Gateway mit dem ICG Update Wizard aktualisieren Siehe IGEL Cloud Gateway (ICG) aktualisieren.
	Keystore des ausgewählten IGEL Cloud Gateway mit dem Update Keystore Wizard aktualisieren Für das Erneuern des Endzertifikats siehe Ein signiertes Zertifikat für den ICG erneuern. Für den Austausch des Stammzertifikats siehe Stammzertifikat für ICG austauschen.
	Ein existierendes IGEL Cloud Gateway zur UMS-Datenbank hinzufügen. Dieses IGEL Cloud Gateway muss erreichbar sein.
	Das ausgewählte IGEL Cloud Gateway permanent aus der UMS-Datenbank entfernen. ⚠ Wenn Sie ein IGEL Cloud Gateway aus der UMS-Datenbank entfernen, können Sie es nicht wieder zur UMS-Datenbank hinzufügen. In den meisten Fällen ist es vorzuziehen, das IGEL Cloud Gateway zu deinstallieren und dann mit dem ICG Remote Installer erneut zu installieren.
	Die Einstellungen des ausgewählten IGEL Cloud Gateway bearbeiten
	Zur Ansicht der ICG-Instanz navigieren
	Limit für Verbindungen zum ICG setzen (ICG 2.02 erforderlich)

Neues IGEL Cloud Gateway verbinden

- **Name**: Anzeigename des Gateway. Die maximale Länge des Namens ist auf 200 Zeichen begrenzt.
- **Host**: DNS-Name oder IP-Adresse des Gateway
- **Port**: TCP-Port, an dem das Gateway lauscht (Standard: 8443)
- **Host (extern)**: Externer DNS-Name/IP-Adresse des Gateway
- **Port (extern)**: TCP-Port, an dem das Gateway nach externen Verbindungen lauscht

- **Proxyserver Einstellungen**:
  - **Kein Proxyserver**: Direkte Verbindung zu ICG
  - **Standard Proxyserver verwenden**: Der unter Proxyserver (see page 641) definierte Standardproxyserver wird verwendet.
  - **Manuelle Proxy Konfiguration**: Einen Proxyserver aus der Liste auswählen

  Wie Sie alle Komponenten für eine Anbindung mit ICG einrichten, lesen Sie in Installation und Einrichtung.

IGEL Cloud Gateway (Instanz)

Menüpfad: **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway > [Anzeigename]**

Hier finden Sie Informationen über ein konfiguriertes Gateway und können die Verbindung herstellen oder trennen.

	Cloud Gateway verbinden
	Cloud Gateway trennen
	Informationen über Cloud Gateway neu laden

Statistik

Eine Übersicht der **Anfragen** durch Geräte erlaubt eine Einschätzung der Serverlast, wie sie sich über den betrachteten Zeitraum verteilt.

▶ Klicken Sie **Historie anzeigen**, um eine skalierbare Ansicht zu öffnen. Sie können mit der Maus in Ausschnitte hereinzoomen oder mittels Mausgeste (nach links ziehen mit gedrückter Maustaste) die Ansicht wiederherstellen.

Globale Konfiguration

Menüpfad: **UMS Administration > Globale Konfiguration**

Unter **Globale Konfiguration** können Sie administrative Aufgaben (see page 597) regeln, Benutzerdaten aus dem Active Directory (see page 657) integrieren, das Universal Firmware Update (1) (see page 559) einrichten und die Lizenzen (see page 560) verwalten.

_____

Lizenzen

Menüpfad: **UMS Administration > Globale Konfiguration > Lizenzen**

Auf diesen Seiten verwalten Sie Lizenzen für die UMS sowie für Geräte, die von der UMS verwaltet werden.

UMS Lizenzen

Menüpfad: **UMS Administration > Globale Konfiguration > Lizenzen**

In diesem Bereich erhalten Sie einen Überblick über die Verfügbarkeit und den Status aller Lizenzen für UMS-Erweiterungen.

Lizenzüberblick

- **Lizenztyp**: Name der lizenzierten UMS-Erweiterung
- **Verfügbare Lizenzen**: Gesamtzahl der in der Lizenzdatei enthaltenen Einheiten
- **Benutzte Lizenzen**: Einheiten der Lizenz, die vom System derzeit in Anspruch genommen werden
- **Lizenzstatus**: Gültigkeit der Lizenz

Registrierte Lizenzen

	Lizenzdatei hinzufügen
	Lizenz löschen
	Inhalt der Lizenzdatei anzeigen

- **Lizenz-ID**: Identifikationsnummer der Lizenz
- **Lizenz registriert am**: Zeitpunkt, an dem die Lizenzdatei auf dem Activation Portal generiert wurde
- **Anzahl**: Gesamtzahl der in der Lizenzdatei enthaltenen Einheiten
- **Kunde**: Kundenname (optional)
- **Dienste**: Lizenzierter Dienst, z.B. IGEL Cloud Gateway
- **Maintenance Subscription**: Berechtigung, Updates der lizenzeierten Erweiterung zu installieren
- **Aktivierungsschlüssel**: Im Activation Portal zur Lizenzgeneriereung verwendeter Schlüssel
- **Testlizenz**: Zeigt an, ob es sich um eine Tetlizenz handelt
- **Ablaufdatum**: Ende des Lizenzzeitraums

Gerätelizenzen

Menüpfad: **UMS Administration > Globale Konfiguration > Lizenzen > Gerätelizenzen**

IGEL Lizenzen

Hier können Sie Lizenzen für Geräte verwalten, beispielsweise für mit UDC3 konvertierte Geräte.

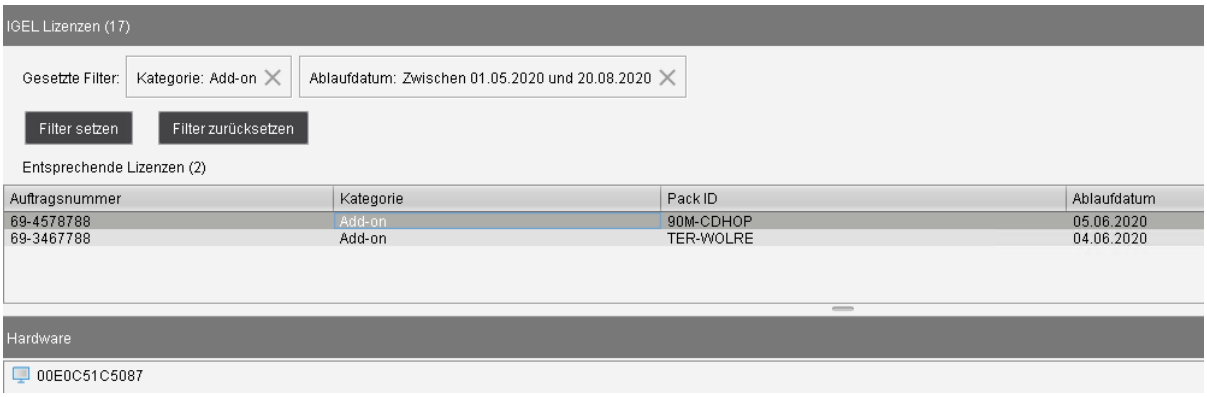
	Lizenzdatei hinzufügen
	Lizenz löschen
	Inhalt der Lizenzdatei anzeigen

- **Filter**: Beschränkt die Listenansicht auf bestimmte Lizenzen:
  - Alle Lizenzen anzeigen
  - Gültige Maintenance Subscriptions anzeigen
  - Abgelaufene Maintenance Subscriptions anzeigen
  - Maintenance Subscriptions anzeigen, welche ablaufen in den nächsten
    - Monaten
    - Tagen
  - Alle Lizenzen eines Thin Clients anzeigen
    - Unit ID
    -  (Blättern im Gerätestrukturbaum)
  - Testlizenzen anzeigen

Spalten der Liste:

- **Auftragsnummer**: Auftragsnummer, unter der die Lizenz bestellt wurde
- **Hardwaretyp**: Merkmal der Hardware, z.B. **macddress**
- **Maintenance Subscription**: Zeigt an, ob eine Subscription besteht.
- **Aktivierungsschlüssel**: Aktivierungsschlüssel, mit dem die Lizenz generiert wurde
- **Testlizenz**: Zeigt an, ob es sich um eine Testlizenz handelt.
- **Ablaufdatum**: Ende des Lizenzzeitraums

Filter setzen / Filter zurücksetzen



Um einen Überblick zu erhalten, der Ihren Bedürfnissen entspricht, können Sie die Anzeige der vorhandenen Lizenzen filtern. Es können maximal 20 000 Lizenzen angezeigt werden.

Sie können einen Filter durch die Kombination verschiedener Kriterien erstellen, oder Sie können für jedes Kriterium einen separaten Filter erstellen. Wenn Sie mehrere Filter erstellt haben, können Sie jeden Filter einzeln entfernen.

- Um einen Filter zu konfigurieren, klicken Sie **Filter setzen**.
- Um alle vorhandenen Filter zu entfernen, klicken Sie **Filter zurücksetzen**.

Die folgenden Kriterien sind verfügbar:

Kategorie
Mögliche Optionen:

- "Alle": Es findet keine Auswahl nach Kategorien statt.
- "Maintenance": Wählt Maintenance-Lizenzen aus.
- "Subscription": Wählt Subscription-Lizenzen aus.
- "Add-on": Wählt Add-on-Lizenzen aus.
- "Evaluierung": Wählt Evaluierungslizenzen aus.

Auftragsnummer: Wählt alle Lizenzen aus, die zur angegebenen Auftragsnummer gehören.

Pack ID: Wählt alle Lizenzen aus, die zum Product Pack mit der angegebenen Pack ID gehören.

Ablaufdatum: Wählt die Lizenzen mit dem angegebenen Ablaufdatum aus.
Mögliche Optionen:

- "Alle"
- "Datumsbereich"
- "Datum"
- "Unendlich"

Unit ID: Wählt die Lizenzen aus, die dem Gerät mit der angegebenen Unit ID zugewiesen sind. Die Unit ID kann mit Klick auf  aus dem Strukturbaum ausgewählt werden.

Tabellenspalten

Auftragsnummer: Auftragsnummer, mit der die Lizenz bestellt wurde

Kategorie: Kategorie, zu der die Lizenz gehört; mögliche Kategorien: "Maintenance", "Subscription", "Add-on" oder "Evaluierung"

Pack ID: ID des Product Packs, zu der die Lizenz gehört

Ablaufdatum: Ablaufdatum der Lizenz

Hardware

Hier können sie Thin Client Listen anzeigen oder für das Activation Portal exportieren sowie UDC2-Lizenzen von einer Smartcard erstellen.

Unit ID-Liste exportieren: Öffnet Export-Wizard

Thin Client-Listen: Öffnet Endgeräteliste mit Filtermöglichkeit

- **Lizenz von der Smartcard ausstellen**: UDC2-Lizenz von der Smartcard erstellen

Verteilung - Lizenzen durch die IGEL UMS Verteilen

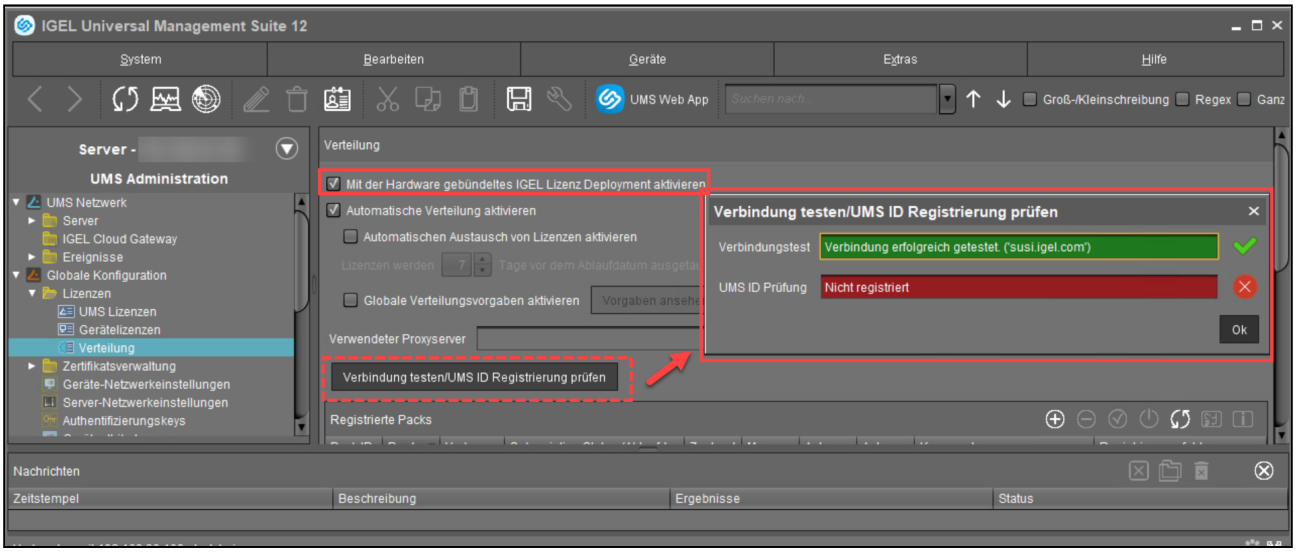
Sie können die automatische Verteilung von Lizenzen durch die IGEL Universal Management Suite (UMS) aktivieren und konfigurieren. Die automatische Lizenzverteilung umfasst Lizenzen für OSC/UDC3, UMA und UD Pocket. Sobald im Handel erhältlich, kann die UMS auch automatisch hardwaregebündelte IGEL-Lizenzen verteilen.

Menüpfad: **UMS Konsole > UMS Administration > Globale Konfiguration > Lizenzen > Verteilung**

Hardware Gebündeltes IGEL Lizenz Deployment

Eine hardware-gebündelte IGEL-Lizenz wird zusammen mit einer von einem IGEL-Hardwarepartner hergestellten Hardware erworben. Sobald diese Art von Lizenz im Handel erhältlich ist, handelt es sich um eine COSMOS PAS (Platform Access Subscription), die auf der Grundlage der Seriennummer des Geräts, mit dem sie verkauft wird, implementiert wird. Die Lizenz kann automatisch über die UMS oder manuell über das IGEL Licensing Portal (ILP) verteilt werden. Die Lizenz kann von der Hardware getrennt und auf einem anderen Gerät verteilt werden.

> ⓘ Sobald sie im Handel erhältlich ist, steht die Funktion der hardware-gebündelten Bereitstellung in UMS 12.2.120 oder höher und für Geräte mit Version 11.08.440 / 12.2.0 oder höher zur Verfügung.



Mit der Hardware gebündeltes IGEL Lizenz Deployment aktivieren

☑ Hardware-gebündelte Lizenzen werden automatisch über die UMS verteilt.

☐ Hardware-gebündelte Lizenzen werden nicht über die UMS verteilt; die Verteilung muss manuell erfolgen. (Standard)

Damit die automatische Verteilung von hardware-gebündelte Lizenzen funktioniert, muss die UMS-ID im ILP registriert werden. Um die Registrierung zu überprüfen, klicken Sie auf **Verbindung testen/UMS ID Registrierung prüfen**.

Automatische Lizenzverteilung

Ab UMS 12 werden Demolizenzen für IGEL OS 12- und IGEL OS 11-Geräte von der automatischen Lizenzverteilung unterstützt.

Voraussetzung für die automatische Lizenzverteilung ist eine Verbindung zwischen der UMS und dem IGEL Lizenzserver sowie dem IGEL Updateserver. Diese Verbindung kann über einen Proxy erfolgen.

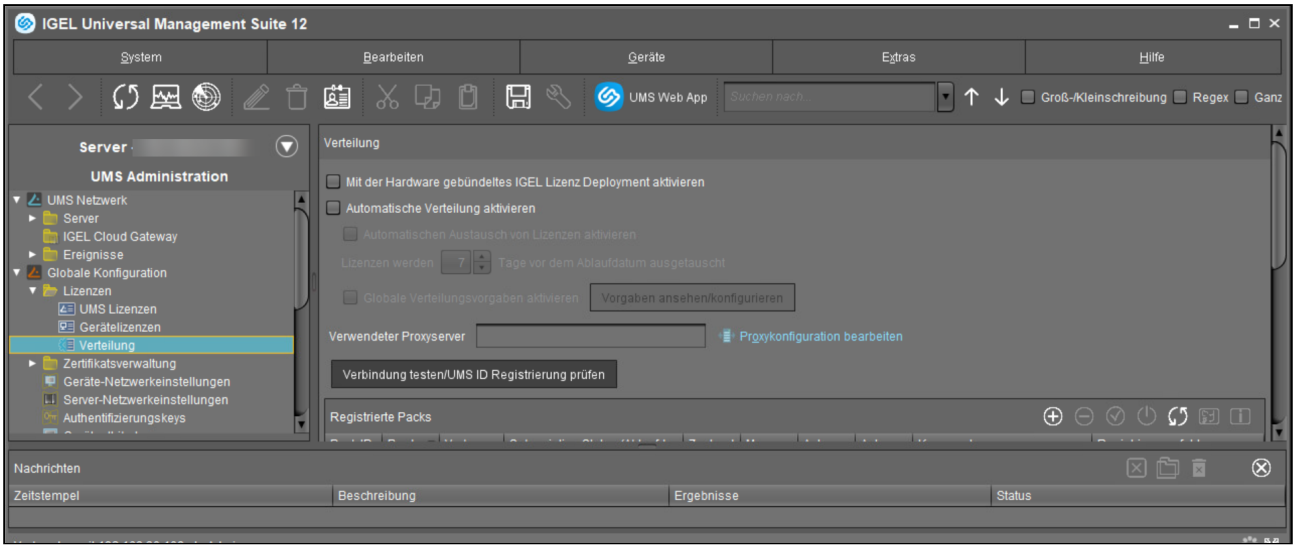
Einzelheiten zu den Vorgängen der automatischen Linzenzverteilung finden Sie unter Intervalle für die automatische Lizenzbereitstellung.

Sind mehrere Product Packs verfügbar, für die geeignete und noch nicht vergebene Lizenzen hinterlegt sind, erfolgt die Auswahl nach folgenden Kriterien:

- Das Product Pack mit den meisten bereits vergebenen Lizenzen wird zuerst verwendet.
- Product Packs mit einem früheren Registrierungsdatum werden vor Product Packs mit einem späteren Registrierungsdatum verwendet.

Sobald eine Lizenz in der UMS registriert ist, speichert die UMS die Lizenz und fügt den Geräteeinstellungen einen Link zum Herunterladen der Lizenz hinzu. Daraufhin sendet die UMS die aktuellen Einstellungen an die Geräte. Wenn die Geräte ihre Einstellungen erhalten haben, laden sie die Lizenzen herunter und starten neu. Nach dem Neustart verfügen die Geräte über alle lizenzierten Features.

Weitere Informationen zur Einrichtung und Nutzung der automatischen Lizenzverteilung finden Sie unter Automatic License Deployment (ALD) einrichten.



Automatische Verteilung aktivieren

☑ Die automatische Lizenzverteilung ist aktiv.

☐ Es erfolgt keine automatische Lizenzverteilung. (Standard)

Automatischen Austausch von Lizenzen aktivieren

☑ Der automatische Austausch von auslaufenden Gerätelizenzen ist aktiviert. Wenn das aktuelle Product Pack nicht erneuert wurde und die aktuelle Gerätelizenz abläuft, wird ein Gerät aus einem anderen Product Pack lizenziert. D.h. es wird geprüft, ob ein Product Pack mit einem späteren Ablaufdatum in der UMS registriert ist (siehe unten Registrierte Packs (see page 569)), und in diesem Fall werden die neuen Lizenzen aus diesem Product Pack an die Geräte verteilt. Die alten Lizenzen werden nicht von den Geräten entfernt.

Geben Sie an, wann die neuen Lizenzen an die Geräte verteilt werden sollen unter **Lizenzen werden [Anzahl] Tage vor dem Ablaufdatum ausgetauscht**.

☐ Der automatische Austausch von auslaufenden Gerätelizenzen ist deaktiviert. (Standard)

Lizenzen werden [Anzahl] Tage vor dem Ablaufdatum ausgetauscht

Legt fest, wie viele Tage vor dem Ablaufdatum eine neue Lizenz bereitgestellt werden soll. (Standard: 7)

Globale Verteilungsvorgaben aktivieren

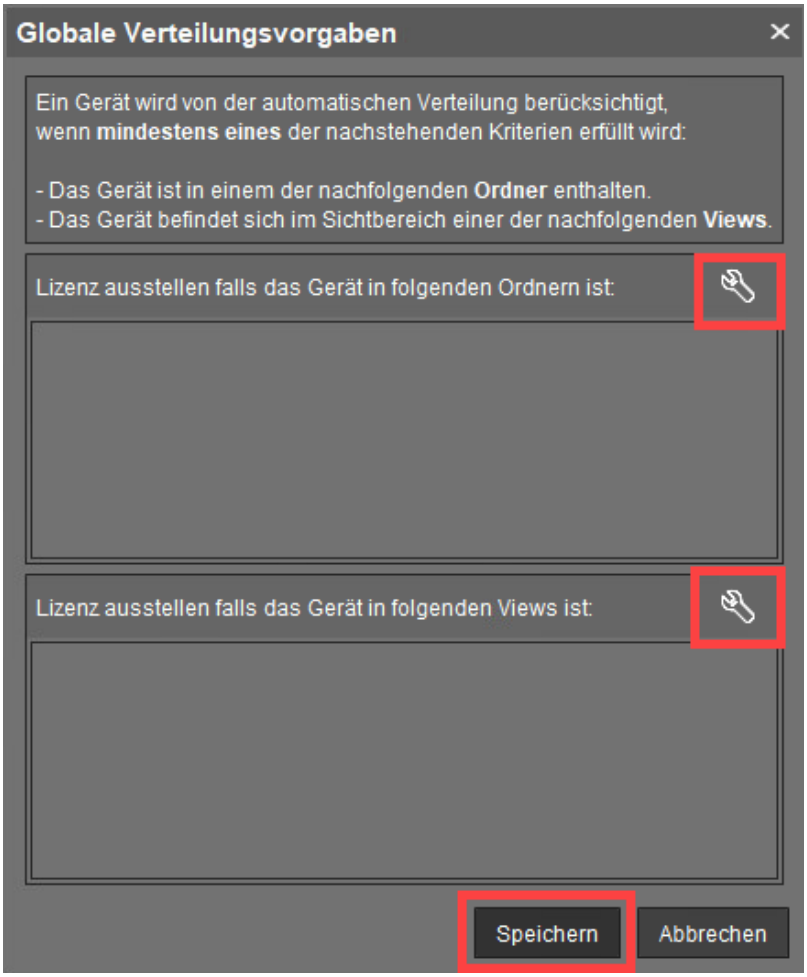
☑ Für die automatische Lizenzverteilung werden nur Geräte berücksichtigt, die die unter **Vorgaben ansehen/konfigurieren** definierten Bedingungen erfüllen. Diese Bedingungen gelten global für die automatische Lizenzverteilung. Sie können jedoch auch Pack-spezifische Verteilungsvorgaben konfigurieren (siehe "Registrierte Packs" unten).

> ⓘ **Globale Verteilungsvorgaben vs. Pack-spezifische Verteilungsvorgaben**
> Die globalen Verteilungsvorgaben geben an, welche Geräte generell für die automatische Lizenzverteilung berücksichtigt werden. Diese Menge an Geräten kann durch die Pack-spezifischen Verteilungsvorgaben weiter eingeschränkt werden. Die Pack-spezifischen Verteilungsvorgaben stellen also eine zusätzliche Einschränkung zu den globalen Verteilungsvorgaben dar.
> Das bedeutet auch, dass ein Gerät, das bereits durch die globalen Verteilungsvorgaben ausgeschlossen wurde, nicht durch die Pack-spezifischen Verteilungsvorgaben zur automatischen Lizenzverteilung "hinzugefügt" werden kann.

☐ Die globalen Verteilungsvorgaben sind deaktiviert. (Standard)

Vorgaben ansehen/konfigurieren

Öffnet einen Dialog, in dem Sie ein oder mehrere Verzeichnisse oder Views als globale Verteilungsvorgaben auswählen können:



Verwendeter Proxy Server

Bezeichnung des aktuell verwendeten Proxys.

Proxykonfiguration bearbeiten

Öffnet einen Dialog zur Auswahl eines Proxys für die Kommunikation mit dem Lizenzserver. Beachten Sie, dass dieser Proxy auch für alle IGEL Cloud Services, einschließlich IGEL Onboarding Service, IGEL Insight Service, IGEL App Portal sowie für UMS as an Update Proxy (see page 889) verwendet wird.

> Ein oder mehrere Proxys müssen erst unter **UMS Administration > Globale Konfiguration > Proxyserver** konfiguriert werden; siehe Proxyserver (see page 641).

Mögliche Optionen:

- **Kein Proxyserver**: Es wird kein Proxyserver verwendet.

- **Standard-Proxyserver verwenden**: Der unter Proxyserver (see page 641) definierte Standardproxyserver wird verwendet.
- **Ausgewählten Proxy verwenden**: Ein Server aus der Liste **Konfigurierte Proxyserver** kann ausgewählt werden.

Verbindung testen/UMS ID Registrierung prüfen

Testet die Verbindung zwischen der UMS bzw. dem Proxy und dem IGEL Lizenzserver sowie dem IGEL Updateserver (http://fwu.igel.com/) und prüft, ob die UMS-ID im IGEL-Lizenzierungsportal (ILP) registriert ist.

Registrierte Packs

In dieser Tabelle werden alle aktuell in der UMS registrierten Product Packs angezeigt. Sie können Product Packs hinzufügen, löschen aktivieren oder deaktivieren.

Suchen nach:	Suche in allen Spalten der Tabelle
	Product Pack hinzufügen
	Product Pack löschen
	Product Pack aktivieren
	Product Pack deaktivieren. Ein deaktiviertes Product Pack wird nicht für das Ausstellen von Lizenzen verwendet.
	Informationen zu allen registrierten Product Packs aktualisieren. Die aktuellen Informationen werden vom Lizenzserver bezogen.
	Zeigt und konfiguriert die Verteilungsvorgaben für das ausgewählte Product Pack. Weitere Informationen finden Sie unter Verteilungsbedingungen konfigurieren.
	Details zum Product Pack anzeigen: • **Attribute**: Zeigt alle Attribute eines Product Packs an. • **Lizenzierte Hardware**: Zeigt alle Geräte an, die mit dem zum Eintrag gehörenden Product Pack lizenziert sind.

Die folgenden Informationen werden angezeigt:

- **Pack ID**: ID des Product Packs

- **Produkt**: Typ des Product Packs
- **Verbrauchte Lizenzen**: Lizenzen, die aktuell in Verwendung sind
- **Subscription Status (Ablaufdatum/Laufzeit)**: Bei neuen Product Packs wird die Gültigkeitsdauer angezeigt, bei aktivierten Product Packs das Ablaufdatum.
- **Ablaufdatum**: Ablaufdatum der Lizenz
- **Zustand**
  Mögliche Zustände:
  - "Aktiv"
  - "Deaktiviert"
- **Manuelle Verteilung**
  Mögliche Zustände:
  - "Aktiv"
  - "Deaktiviert"
- **Automatische Verteilung**
  Mögliche Zustände:
  - "Aktiv"
  - "Aktiv (mit Bedingung)"
  - "Deaktiviert"
- **Automatische Verbreitungsvorgabe**: Konfiguriert die Verteilungsvorgaben für das ausgewählte Product Pack. Weitere Informationen finden Sie unter Verteilungsbedingungen konfigurieren.
- **Kommentar**: Product Pack-Kommentare, die im IGEL Lizenz-Portal erstellt wurden
- **Registrierungsfehler**: Wenn die Registrierung eines Product Packs fehlgeschlagen ist, wird die Fehlermeldung hier angezeigt.

Ausgeführte Aktionen

In diesem Bereich werden die zuletzt durchgeführten Aktionen angezeigt.

	Einträge löschen, die älter sind als ein bestimmtes Datum
	Ausgewählte Einträge löschen
	Anzeige aktualisieren
	Details zur ausgewählten Aktion anzeigen

Die folgenden Informationen werden angezeigt:

- **Zeit**: Zeitpunkt, an dem die Aktion durchgeführt wurde
- **Aktion**: Bezeichnung der Aktion
- **Verwendete Pack ID**: Product Pack, dem die Lizenz zugeordnet ist
- **Zahl der betroffenen Geräte**: Anzahl der Geräte, für die eine Lizenz ausgestellt wurde.
- **Resultat**: Ergebnis der Aktion
  Mögliche Resultate:
  - "Erfolgreich"
  - Fehlermeldung

- Erfolgreich
- (Fehlermeldung)

Zertifikatsverwaltung

Menüpfad: **UMS Administration > Globale Konfiguration > Zertifikatsverwaltung**

Hier können Sie Zertifikate für die Kommunikation mit Engeräten, für die Kommunikation über den Web-Port (Standard: 8443) und für die Kommunikation mit dem IGEL Cloud Gateway (ICG) verwalten.

Gerätekommunikation

Im Bereich **Gerätekommunikation** können Sie Zertifikate für die Kommunikation zwischen IGEL Universal Management Suite (UMS) und Geräten verwalten. Das vorkonfigurierte Zertifikat, das den **Keystore alias** "tckey" hat, wird standardmäßig verwendet, wenn keine Änderungen vorgenommen werden.

Sie können ein anderes Zertifikat als Standard setzen; wenn Sie dies tun, werden alle neu registrierten Geräte dieses Zertifikat verwenden, und bereits registrierte Geräte werden ihr zuvor verwendetes Zertifikat durch das neue Standardzertifikat ersetzen.

Keine Unterstützung

Zertifikatsketten und abgelaufene Zertifikate können nicht importiert werden. Zertifikate, die den MD5-Algorithmus verwenden, werden auch nicht unterstützt.

Menüpfad: **UMS Administration > Globale Konfiguration > Zertifikatsverwaltung > Gerätekommunikation**

Die UMS überprüft alle 5 Minuten, ob das Zertifikat auf dem Gerät und das Standardzertifikat noch identisch sind.

Wenn ein Gerät das Standardzertifikat nicht unterstützt, überprüft die UMS jedes Zertifikat daraufhin, ob es unterstützt wird; dabei beginnt sie am oberen Ende der Liste. Wenn kein geeignetes Zertifikat gefunden wird, wird das Gerät nicht registriert.

Wenn Sie ein Zertifikat im Bereicht **Zertifikatsverwaltung** selektieren, werden alle Geräte, die dieses Zertifikat verwenden, im Bereich **Geräte, welche derzeit das selektierte Zertifikat benutzen (**<Anzahl>**)** angezeigt.

High Availability

Wenn Sie die UMS in einem High-Availability-Netzwerk (HA) betreiben und Änderungen bei Zertifikaten vornehmen (Schlüsselpaar importieren, neues Schlüsselpaar generieren, Zertifikat löschen oder aktivieren/deaktivieren, Priorität eines Zertifikats ändern), wird ein neues Netzwerktoken generiert. Sie müssen einen Speicherort festlegen, in dem das neue Netzwerktoken gespeichert werden soll. Die Änderungen werden dann innerhalb eines HA-Netzwerks automatisch synchronisiert; ein Neustart von IGEL RMGUIServer/igelRMserver-Diensten wird nicht benötigt.

Von einem Backup wiederherstellen

Prüfen Sie bei der Wiederherstellung von einem Backup, ob das Backup Zertifikate enthält, die sich von den aktuell verwendeten Zertifikaten unterscheiden. Wenn das der Fall ist, müssen alle Geräte, die vor der Wiederherstellung registriert waren, erneut registriert werden.

UMS Update

Zertifikate werden bei einer Aktualisierung der UMS nicht überschrieben.

Mögliche Aktionen

 Zertifikat aus einer Datei importieren. Der private Schlüssel muss in der Datei enthalten sein. Der Dateipfad wird unter **Keystore Datei** angegeben und das Passwort unter **Keystore Passwort**. Wenn die UMS den Signaturalgorithmus nicht unterstützt, wird das Zertifikat nicht importiert.

Unterstützte Signaturalgorithmen

Die folgenden Signaturalgorithmen werden unterstützt: SHA512withRSA, SHA384withRSA, SHA256withRSA, SHA1withRSA, SHA256withDSA und SHA1withDSA.

Die Verwendung von Zertifikaten mit SHA1-Signaturalgorithmen wird aus Sicherheitsgründen NICHT empfohlen.

Unterstützte Keystore-Typen

Die folgenden Keystore-Typen werden unterstützt: JCEKS, JKS, PKCS#12, BKS-V1, BKS, UBER und BCFKS.

 Zertifikat generieren.

 Ausgewähltes Zertifikat löschen.

Löschen Sie kein Zertifikat, das von einem Gerät verwendet wird; ansonsten kann die UMS mit diesem Gerät nicht mehr kommunizieren.

 Ausgewähltes Zertifikat in der Liste nach oben verschieben, um seine Priorität zu erhöhen.

Wenn Sie das ausgewählte Zertifikat an die oberste Position der Liste verschieben, wird es zum Standardzertifikat. Die Änderung des Standardzertifikats wird in einer Hintergrundaufgabe der UMS an die Geräte weitergegeben. Diese Aufgabe ersetzt das Zertifikat auf allen Geräten, die mit diesem Zertifikat kompatibel sind, und läuft alle 5 Minuten.

 Ausgewähltes Zertifikat in der Liste nach unten verschieben, um seine Priorität zu erniedrigen.

 Ausgewähltes Zertifikat aktivieren. Wenn ein Zertifikat aktiviert ist, kann es für die Kommunikation zwischen UMS und Geräte verwendet werden.

 Ausgewähltes Zertifikat deaktivieren. Ein Zertifikat wird nicht verwendet, wenn ein neues Gerät registriert wird. Wenn ein Zertifikat deaktiviert wird, während es in Verwendung ist, ist die Kommunikation zwischen UMS und Geräte noch möglich. Wenn nur 1 Zertifikat aktiv ist, kann dieses Zertifikat nicht deaktiviert werden.

 Ausgewähltes Zertifikat exportieren.

 Schlüsselpaar des ausgewählten Zertifikats exportieren.

 Inhalt des ausgewählten Zertifikats anzeigen.

Web

Menüpfad: **UMS Administration > Globale Konfiguration > Zertifikatsverwaltung > Web**

Überblick

Hier können Sie die Zertifikate für die Kommunikation über den Web-Port (Standard: 8443) verwalten.

Der Web-Port wird für die folgenden Aufgaben verwendet:

- Geräteverwaltung und -kommunikation für Geräte mit IGEL OS 12
- Daten für die Endgeräte bereitstellen (WebDAV usw.)
- Daten für andere Server bereitstellen (High Availability; WebDAV usw.)
- Daten für die UMS Web App bereitstellen
- Einen Einstiegspunkt für IMI und WebStart bereitstellen

Verwendung

- UMS Web App: Zertifikate für den Browser bereitstellen; siehe UMS Web App: The Browser Displays a Security Warning (Certificate Error) (see page 174)
- Wenn Sie eine alternative Zertifikatskette anstelle der Vorinstallierten benötigen: siehe Using Your Own Certificates for Communication over the Web Port (Default: 8443) (see page 125)

> Neue Stamm-Webzertifikate werden auf IGEL OS 12 Geräten bei einem Neustart bereitgestellt, siehe Abschnitt "If You Exchange a Root Web Certificate for IGEL OS 12 Devices" unter Using Your Own Certificates for Communication over the Web Port (Default: 8443) (see page 125).

Mögliche Aktionen

Öffnet den Dialog **Automatische Zertifikatserneuerung bearbeiten**, um die automatische Zertifikatserneuerung umzuschalten.

Der private Schlüssel des Elternzertifikats (Stamm-CA oder Zwischen-CA) muss bekannt sein. Das erneuerte Zertifikat wird den Servern automatisch zugewiesen.

Mögliche Optionen:

- **Automatische Zertifikatserneuerung AKTIVIERT**: Die Endzertifikate werden gemäß der unter **Benutzte End-Zertifikate werden [Anzahl] Tage vor ihrem Ablauf verlängert** angegebenen Zahl erneuert.
- **Automatische Zertifikatserneuerung DEAKTIVIERT**: Die Endzertifikate werden nicht automatisch verlängert.

 Erstellt ein Stammzertifikat.

 Erstellt ein signiertes Zertifikat vom aktuell ausgewählten CA-Zertifikat (Stammzertifikat oder Zwischenzertifikat).

 Entfernt das ausgewählte Zertifikat von der UMS. Nur Zertifikate, die aktuell nicht in Verwendung sind, können entfernt werden.

 Erneuert das ausgewählte Zertifikat; der Dialog **Signiertes Zertifikat generieren** wird geöffnet.

Alle Einstellungen außer dem Ablaufdatum (**Gültig bis**) können belassen werden. Der öffentliche Schlüssel des Elternzertifikats (Stamm-CA oder Zwischen-CA) muss bekannt sein. Außerdem muss das Ablaufdatum des Elternzertifikats später sein als das neue Ablaufdatum des Endzertifikats.

 Zeigt den Inhalt des ausgewählten Zertifikats an.

 Importiert ein Stamm-CA-Zertifikat.

 Importiert ein signiertes Zertifikat, für das das aktuell ausgewählte Zertifikat ein Elternzertifikat ist (Stamm-CA oder Zwischen-CA).

 Importiert den entschlüsselten privaten Schlüssel für das ausgewählte Zertifikat.

⚠ Der private Schlüssel wird beim Speichern in der UMS-Datenbank wieder verschlüsselt.

 Importiert eine Zertifikatskette aus einem Keystore.

 Exportiert ein Zertifikat und die dazugehörigen Kindzertifikate als Zertifikatskette in einen Keystore.

 Weist das ausgewählte Zertifikat einem oder mehreren Servern zu. Weitere Informationen finden Sie unter Using Your Own Certificates for Communication over the Web Port (Default: 8443) (see page 125).

Cloud Gateway

Menüpfad: **UMS Administration > Globale Konfiguration > Zertifikatsverwaltung > Cloud Gateway**

Überblick

Hier können Sie die Zertifikate für die Kommunikation zwischen dem IGEL Cloud Gateway (ICG) und den Endgeräten verwalten.

Für eine eingehende Beschreibung, wie man alle Komponenten für eine Verbindung zum ICG aufsetzt, lesen Sie Installation und Einrichtung.

Verwendung

- Ein signiertes Zertifikat für den ICG erneuern
- Stammzertifikat für ICG austauschen

Mögliche Aktionen

 Erstellt ein Stammzertifikat.

 Importiert ein Stamm-CA-Zertifikat.

 Erstellt ein signiertes Zertifikat (Stammzertifikat oder Zwischenzertifikat) vom ausgewählten CA-Zertifikat.

 Entfernt das ausgewählte Zertifikat von der UMS. Nur Zertifikate, die aktuell nicht in Verwendung sind, können entfernt werden.

 Exportiert das ausgewählte Endzertifikat und die vollständige dazugehörige Zertifikatskette in einen Keystore im für den IGEL Cloud Gateway spezifischen Keystore-Format.

 Zeigt den Inhalt des ausgewählten Zertifikats an.

 Führt zu dem IGEL Cloud Gateway, der das ausgewählte Zertifikat verwendet.

Stammzertifikat generieren

Name: Name im Stammzertifikat (common name, CN).

Ihre Organisation: Organisation, Firma, Regierungsbehörde.

Ihre Lokalität (oder Identifier): Standort der Organisation.

Ihr Ländercode (zwei Buchstaben): Country Code nach ISO 3166, z.B. DE für Deutschland.

Gültig bis: Lokales Datum, an den das Zertifikat abläuft (Standard: in 20 Jahren).

Stammzertifikat importieren

Das Fenster zur Dateiauswahl öffnet sich, mit dem Sie die Zertifikatsdatei auswählen können; diese muss im Format PEM sein.

Signiertes Zertifikat generieren

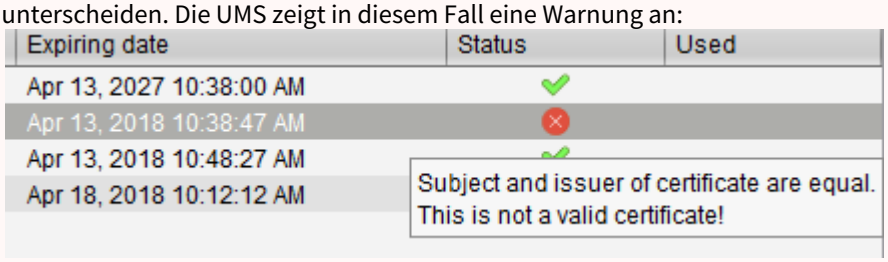
Name: Name im Stammzertifikat (common name, CN).

Ihr Vor- und Nachname: Name Zertifikatseigentümers.

Ihre Organisation: Organisation, Firma, Regierungsbehörde.

Ihre Lokalität (oder Identifier): Standort der Organisation.

Der Name in einem signierten Zertifikat muss sich von dem im Stammzertifikat, mit dem es signiert ist, unterscheiden. Die UMS zeigt in diesem Fall eine Warnung an:



Ihr Ländercode (zwei Buchstaben): Country Code nach ISO 3166, z.B. DE für Deutschland.

Hostname und/oder IP des Zielservers für das Zertifikat: Hostname(n) und IP-Adresse(n), für die das Zertifikat gültig ist. Mehrfacheinträge sind möglich und sollten durch Semikolon getrennt sein. Um ein Wildcard-Zertifikat zu generieren, verwenden Sie das Sternchen, z. B. *.example.com.

Gültig bis: Lokales Datum, an den das Zertifikat abläuft. (Standard: in einem Jahr)

Zertifikats-Typ
Mögliche Optionen:

- **CA-Zertifikat**: Das Zertifikat kann verwendet werden, um andere Zertifikate zu signieren, kann aber nicht vom ICG verwendet werden.
- **End Entity**: Das Zertifikat kann vom ICG verwendet werden, nicht aber, um andere Zertifikate zu signieren.

Kontextmenü (Stammzertifikat)

Signiertes Zertifikat generieren: Sammelt die Zertifikatsdaten und signiert sie mit dem ausgewählten Stammzertifikat.

Signiertes Zertifikat importieren: Importiert ein Zertifikat, das bereits außerhalb der UMS von der importierten CA signiert wurde.

Entschlüsselten privaten Schlüssel importieren: Importiert eine Datei mit einem privaten Schlüssel.

Wenn der private Schlüssel mit einer Passphrase geschützt ist, müssen Sie ihn auf der Kommandozeile mit OpenSSL entschlüsseln, bevor Sie ihn importieren: `openssl rsa -in encrypted.key -out decrypted.key`

Zertifikat löschen: Löscht das Zertifikat aus der UMS.

Zertifikatskette im IGEL Cloud Keystore Format exportieren: Erzeugt eine Datei für das ICG-Installationsprogramm.

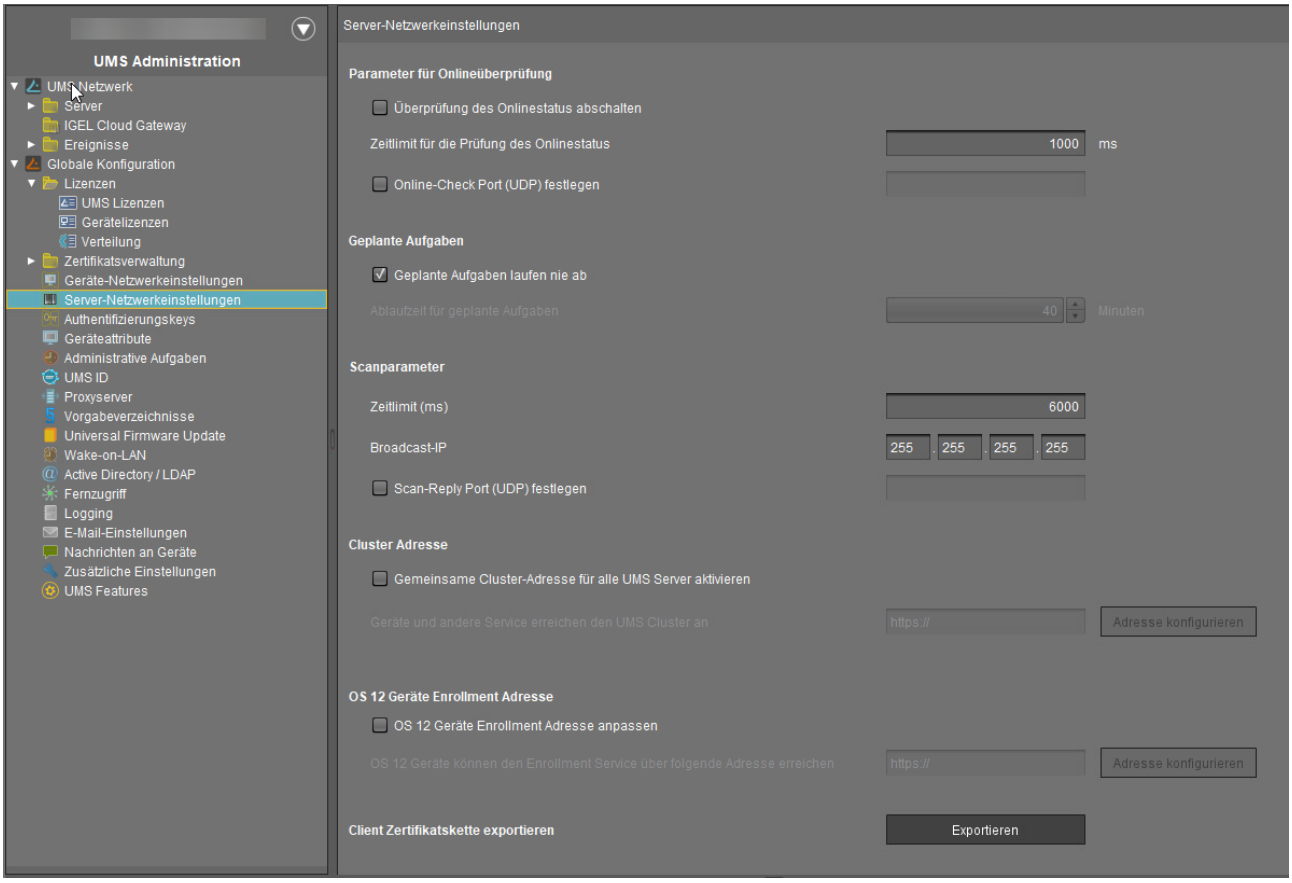
Zertifikat exportieren: Exportiert das Zertifikat.

Inhalt des Zertifikats anzeigen: Zeigt den Inhalt des Zertifikats in einem Textfenster an.

Server-Netzwerkeinstellungen in der IGEL UMS

In diesem Bereich der IGEL Universal Management Suite (UMS) Konsole können Sie Einstellungen für die Prüfung des Onlinestatus Ihrer Geräte sowie Scanparameter konfigurieren, die Aktivierung der Distributed UMS-Funktion vornehmen, die Cluster-Adresse für die Lastverteilung bestimmter Geräteanfragen angeben, usw.

Menüpfad: **UMS Konsole > UMS Administration > Globale Konfiguration > Server-Netzwerkeinstellungen**



Parameter für Onlineüberprüfung

Überprüfung des Onlinestatus abschalten

☑ Die Onlineprüfung ist deaktiviert.

☐ Die Onlineprüfung ist aktiviert. (Standard)

Zeitlimit für die Prüfung des Onlinestatus

Zeitlimit in Millisekunden, wie lange auf die Antwort einer Onlinestatus-Abfragenachricht gewartet wird. Die UMS versucht, alle Geräte zu kontaktieren, die in der UMS Konsole gerade sichtbar sind. Jedes Gerät in diesem Bereich muss in der vorgegebenen Zeit auf die Statusanfrage antworten oder wird als "offline" markiert. Minimum: 100; Maximum: 10000; Standard: 1000

Geänderte Werte bei Update

Der maximale und der minimale Wert sowie der neue Standardwert wurden mit UMS 6.04.100 eingeführt. Wenn Sie von einer älteren Version auf UMS 6.04.100 aktualisiert haben, wird der Wert wie folgt behandelt:

- Wenn der Wert zwischen 100 und 10.000 war, bleibt er unverändert.
- Wenn der Wert niedriger als 100 war, wird er auf 100 gesetzt.
- Wenn der Wert auf den alten Standardwert 100 gesetzt war, wird er auf den neuen Standardwert 1.000 gesetzt.
- Wenn der Wert höher als 10.000 war, wird er auf 10.000 gesetzt.

Online-Check Port (UDP) festlegen

☑ Sie geben den Port an, an den die Geräte ihre Antwort schicken, wenn die UMS deren Online-Status prüft.

☐ Die UMS wählt einen freien Port aus. (Standard)

Geplante Aufgaben

Geplante Aufgaben laufen nie ab

☑ Kein Zeitlimit für geplante Aufgaben (Standard)

Ablaufzeit für geplante Aufgaben

Zeit in Minuten, nach der eine geplante Aufgabe ablaufen soll. (Standard: 40)

Scanparameter

Zeitlimit (ms)

Zeit in Millisekunden, die die UMS auf eine Antwort auf Scanpakete warten soll. (Standard: 6000)

Broadcast-IP

Broadcast-Adresse, die für Scanpakete verwendet wird. Sie wird nur zum Scannen des lokalen Netzwerks verwendet. Wenn IP-Bereiche genutzt werden, werden die UDP-Pakete an jeden Client im IP-Bereich versendet. (Standard: 255.255.255.255)

Scan-Reply Port (UDP) festlegen

☑ Sie legen den Port fest, an den die Geräte ihre Antwort schicken, wenn die UMS nach Geräten scannt.

☐ Die UMS wählt einen freien Port aus. (Standard)

Cluster-Adresse

In IGEL UMS High Availability- und Distributed UMS-Installationen können Sie die Cluster-Adresse verwenden, um den eingehenden Datenverkehr auszugleichen.

- Die Cluster-Adresse dient nur zur Kommunikation über den Web-Serverport (see page 709) (Standard: 8443).
- SSL kann auf dem Reverse Proxy / externen Load Balancer (siehe NGINX: Example Configuration for as Reverse Proxy in IGEL OS with SSL Offloading (see page 19)) oder auf dem UMS Server terminiert werden.

Gemeinsame Cluster-Adresse für alle UMS Server aktivieren

☑ Die Adresse und Port, die durch Klicken auf **Adresse konfigurieren** definiert wurden, werden für die folgenden HTTPS-Anfragen von Geräten verwendet:

- Dateiübertragung von der UMS an IGEL OS 11-Geräte
- Onboarding und Gerätekommunikation von IGEL OS 12-Geräten
- Herunterladen von Apps für IGEL OS 12-Geräte, wenn **Apps von der UMS beziehen** unter **UMS Web App > Apps > Einstellungen**  **> UMS as an Update Proxy** eingestellt ist

Die Cluster-Adresse hat KEINE Auswirkungen auf:

- das Herunterladen von Firmwareupdates für IGEL OS 11-Geräte
- die Gerätekommunikation mit den UMS Servern (IGEL OS 11-Geräte)
- die interne Kommunikation zwischen den UMS Servern (inkl. der WebDAV-Synchronisation zwischen den UMS Servern)
- IGEL Cloud Gateway-Kommunikation, d.h. Geräte, die über ICG mit der UMS verbunden sind, verwenden keine Cluster-Adresse

☐ Die Cluster-Adresse wird nicht verwendet. (Standard)

Wenn definiert, wird die **Öffentliche Adresse** für HTTPS-Anfragen von Geräten verwendet, wenn keine **Cluster-Adresse** festgelegt wurde. Weitere Informationen zur Öffentlichen Adresse finden Sie unter Server - Informationen zu Ihrem UMS Server anzeigen (see page 551).

Geräte und andere Service erreichen den UMS Cluster an

Die Adresse wird durch die folgenden Parameter definiert. Die Parameter werden in einem Dialogfeld angezeigt, wenn Sie auf **Adresse konfigurieren** klicken:

- **FQDN des Clusters**

  FQDN Ihres externen Load Balancers / Reverse Proxys wie NGINX, Citrix Netscaler usw. Die maximale Länge ist auf 255 Zeichen beschränkt.

Wenn der Clusteradresse ein Reverse Proxy / Load Balancer zugewiesen ist, kann dieser sowohl externen als auch internen Netzwerkverkehr verarbeiten. Für Informationen zu Clusteradresse und FQDNs siehe auch Troubleshooting: Error 38 during the Onboarding of an IGEL OS 12 Device.

- **Port**

  Port Ihres externen Load Balancers / Reverse Proxys

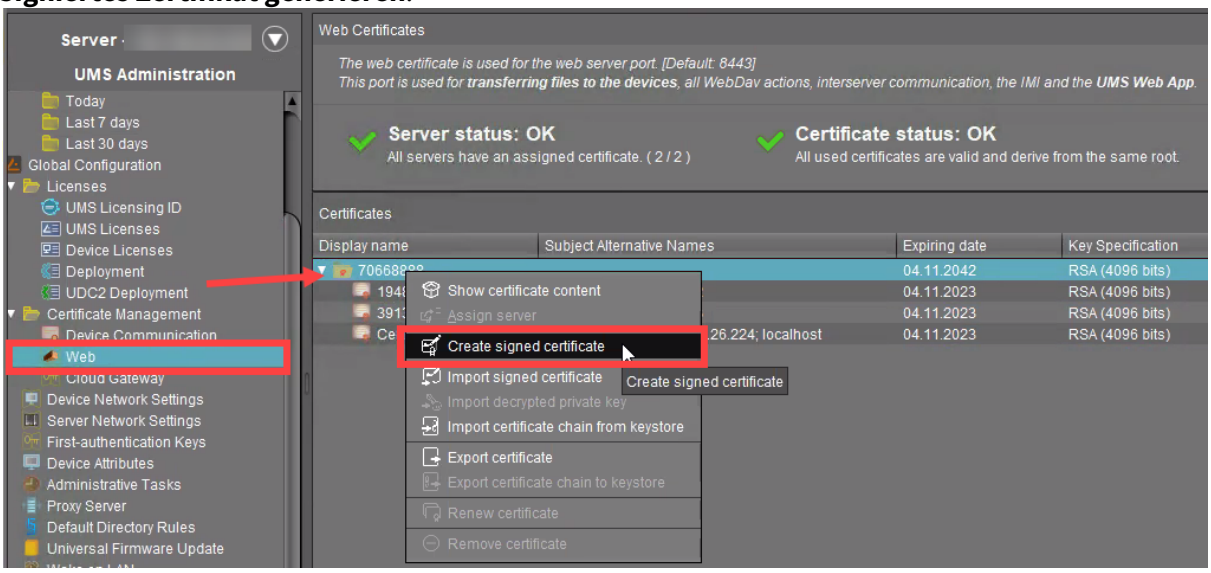
Konfigurieren Sie ein Webzertifikat für alle Server...

Wenn Sie eine UMS HA- oder Distributed UMS-Installation haben und die Cluster-Adresse konfiguriert haben, müssen Sie ein Webzertifikat für alle Server definieren:

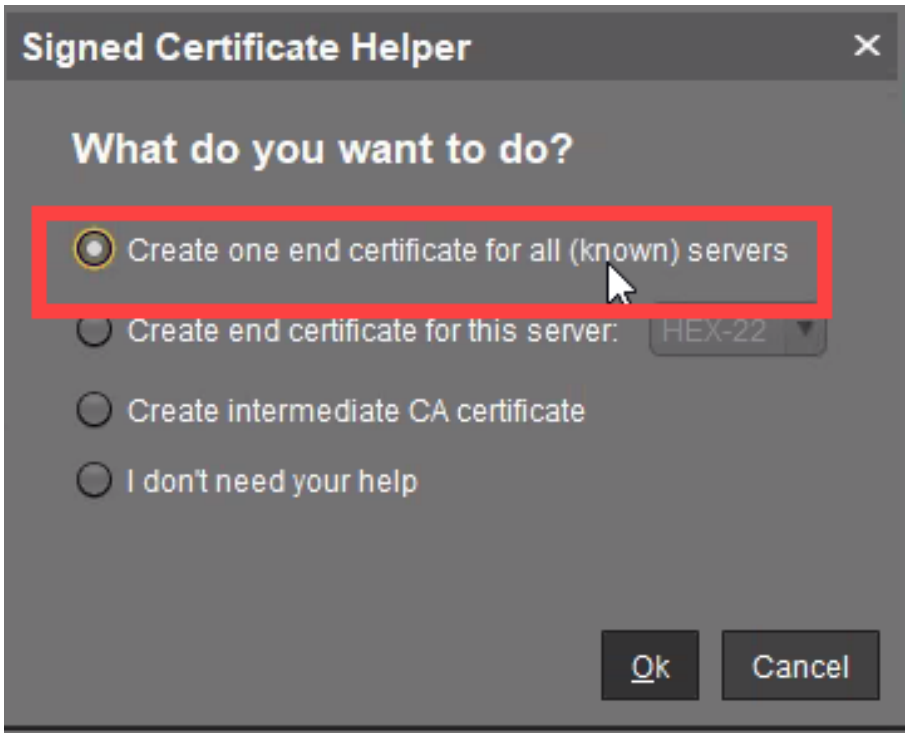
- Das Zertifikat muss die Cluster-Adresse und alle Serveradressen enthalten
- Das Zertifikat muss allen Servern zugewiesen werden

Um ein Webzertifikat für alle Server zu definieren, gehen Sie wie folgt vor:

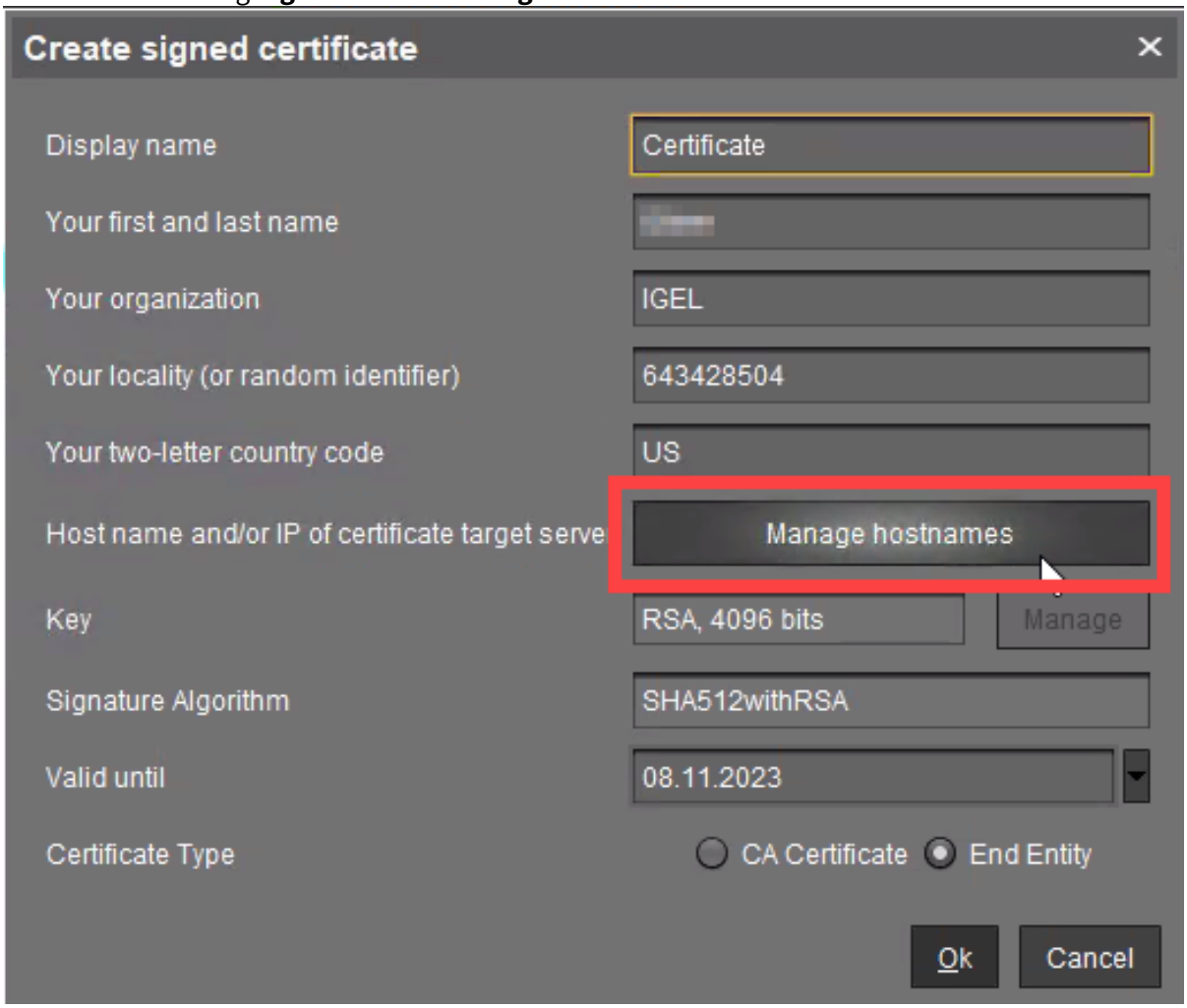
1. Wählen Sie in der **UMS Konsole > UMS Administration > Globale Konfiguration > Zertifikatsverwaltung > Web** das Stammzertifikat aus und klicken Sie im Kontextmenü auf **Signiertes Zertifikat generieren**.



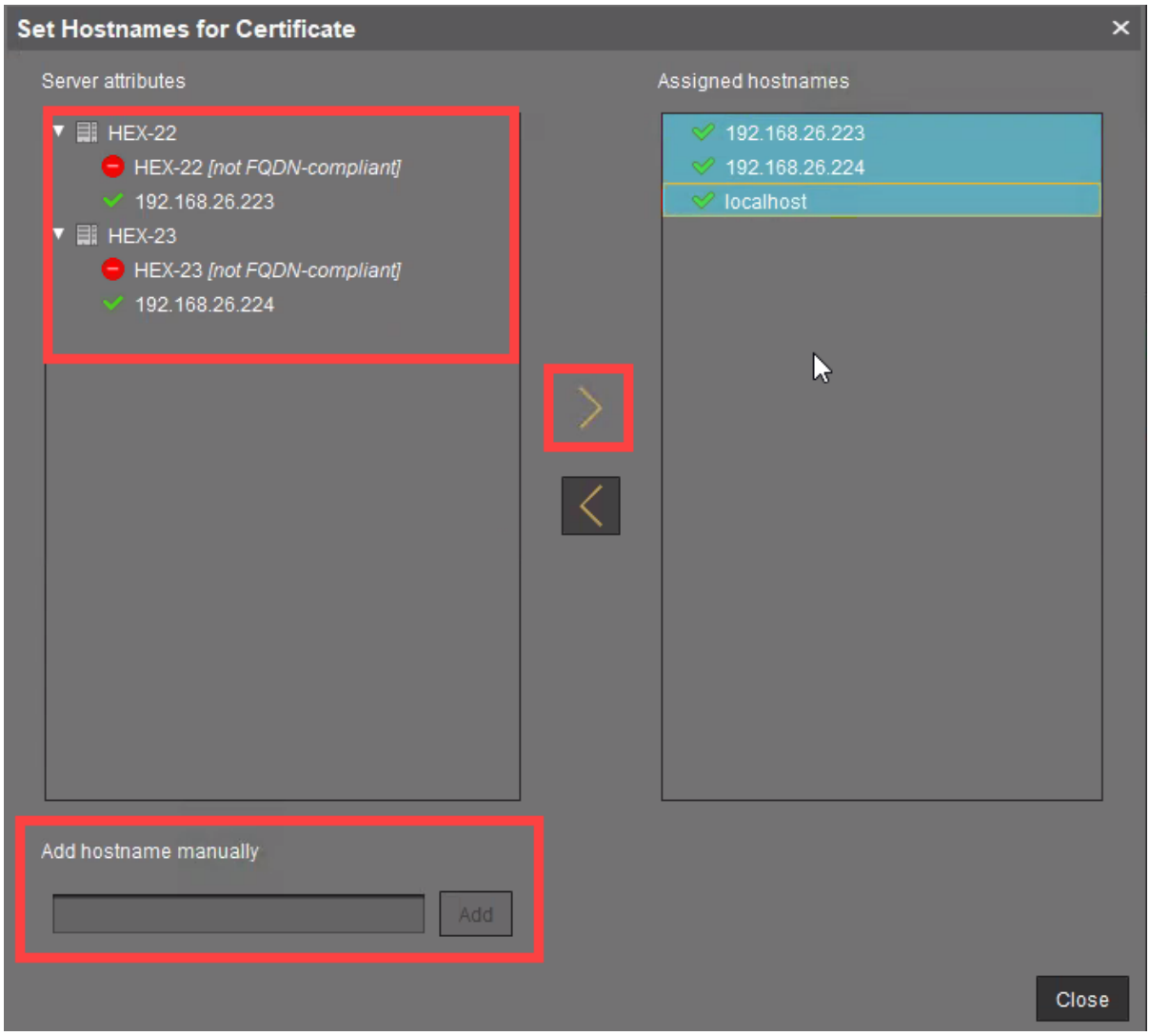
2. Wählen Sie im Dialog **Signierte Zertifikate | Vorauswahl** die Option **Ein Endzertifikat für alle (bekannten) Server erstellen** aus.


Signed Certificate Helper
What do you want to do?
Create one end certificate for all (known) servers
Create end certificate for this server:
HEX-22
Create intermediate CA certificate
I don't need your help
Ok
Cancel

3. Klicken Sie im Dialog **Signiertes Zertifikat generieren** auf **Hostnamen verwalten**.

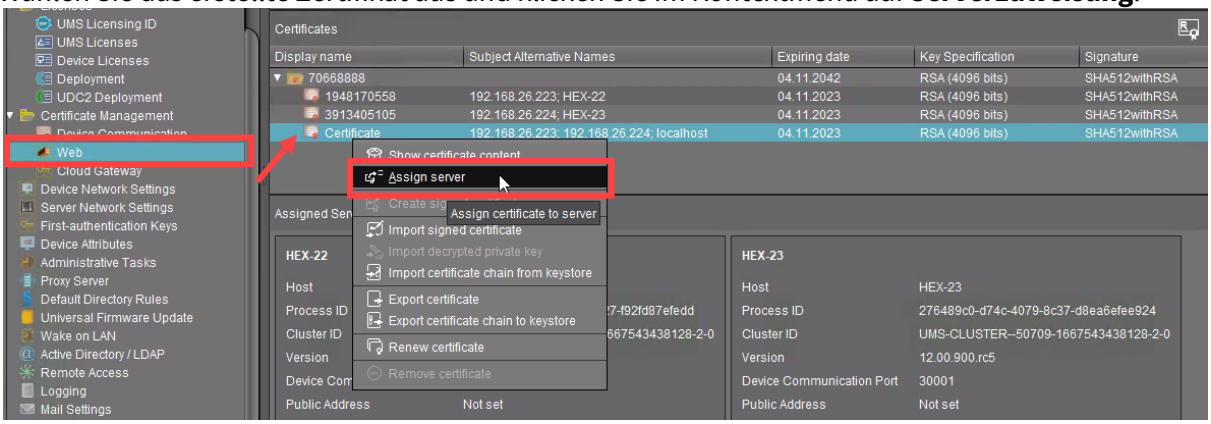


4. Prüfen Sie im Dialog **Hostnamen im Zertifikat hinterlegen**, ob unter **Zugewiesene Hostnamen** die Cluster-Adresse, "localhost", alle IP-Adressen und FQDNs (Fully Qualified Domain Names), unter denen Ihre Server erreichbar sind, angezeigt werden. Falls nicht, fügen Sie die fehlenden IP-Adressen und FQDNs unter **Hostnamen manuell hinzufügen** hinzu.

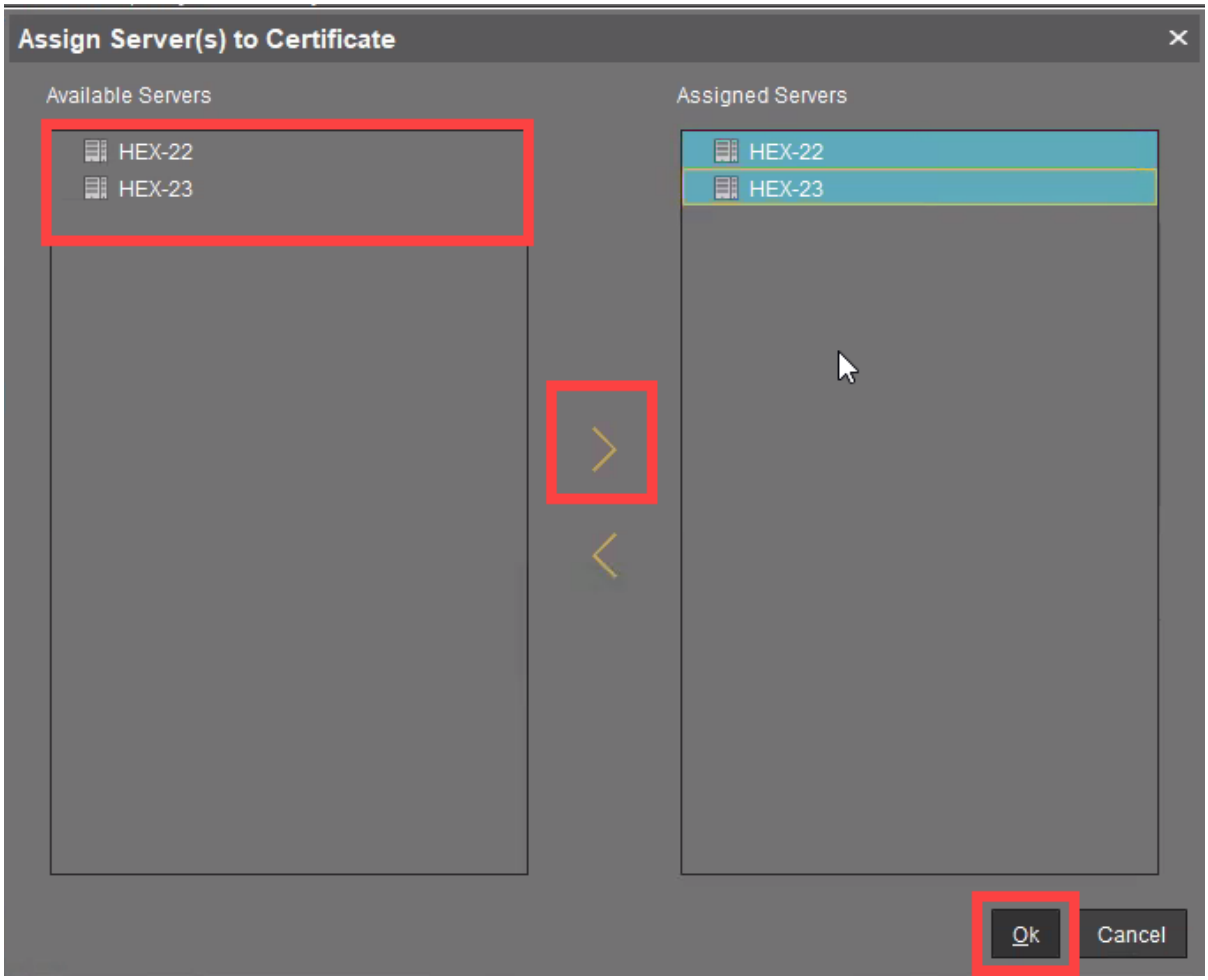


5. Schließen Sie den Dialog **Signiertes Zertifikat generieren** mit **Ok**.
   Das signierte Serverzertifikat wird erstellt.

6. Wählen Sie das erstellte Zertifikat aus und klicken Sie im Kontextmenü auf **Serverzuweisung**.



7. Weisen Sie das Zertifikat allen Servern zu.



OS 12 Geräte Enrollment Adresse

> Diese Konfiguration ermöglicht die Trennung des Endpunkts für das Geräte-Onboarding vom Websocket-Endpunkt (Verwaltung). Diese Option kann für die Implementierung eines Reverse-Proxys/externen Load Balancers ohne optionale Option zur Überprüfung des Client-Zertifikats erforderlich sein, wie z. B. Azure Application Gateway. Für weitere Informationen, siehe Azure Application Gateway: Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading (see page 21).

OS 12 Geräte Enrollment Adresse anpassen

☑ Die Adresse und der Anschluss, die durch Klicken auf **Adresse konfigurieren** definiert wurden, werden für das onboarding des Geräts verwendet.

☐ Die Cluster-Adresse wird für das Onboarding von Geräten in der Reverse-Proxy- / externen Load Balancer-konfiguration verwendet. (Standard)

OS 12 Geräte können den Enrollment Service über folgende Adresse erreichen

Die Adresse, die durch die Parameter definiert ist, auf die durch Anklicken von **Adresse konfigurieren**:

- **FQDN oder IP Adresse**

  FQDN des konfigurierten Listeners für das Geräte-Onboarding.

- **Port**

  Port des konfigurierten Listeners für das Onboarding von Geräten.

- **Pfad Präfix**

  Pfad Präfix zum EST-Dienst. Der definierte Pfad im EST-Protokoll lautet ".well-known/est". Dieses Präfix sollte verwendet werden, um ihn anzupassen. Beispiel: **/device-connector/device**/.well-known/est
  Dieser Wert muss nur gesetzt werden, wenn der Pfad angepasst wurde. Der Standardwert ist leer.

Client Zertifikatskette exportieren

Klicken Sie auf **Exportieren** um die Client-Zertifikatskette zu exportieren.

> Sie benötigen die Client-Zertifikatskette, um den Reverse-Proxy / externen Load Balancer zu konfigurieren. Für weitere Informationen siehe IGEL Universal Management Suite Network Configuration (see page 17).

UMS High Availability / Distributed UMS

Distributed UMS aktiviert (Neustart der UMS Server nach Änderung notwendig)

☑ Die Standalone UMS Server funktionieren so, als ob sie als High Availability-Umgebung installiert wären, wenn sie mit derselben externen Datenbank verbunden sind. Die Nachrichten zwischen den UMS Servern werden über Datenbankeinträge übertragen. Ausführliche Informationen über die Distributed UMS finden Sie unter IGEL UMS Installation (see page 246).

Informationen zur Installation der Distributed UMS oder zur Erweiterung einer bestehenden UMS Standardinstallation auf die Distributed UMS finden Sie unter Distributed IGEL UMS installieren (see page 275).

Wenn Sie eine UMS High Availability-Installation haben, ist das Kontrollkästchen **Distributed UMS aktiviert (Neustart der UMS Server nach Änderung notwendig)** nicht verfügbar.

☐ Die Distributed UMS ist deaktiviert. (Standard)

Wenn Sie die Distributed UMS-Funktion aktiviert haben und über mehrere UMS Server verfügen, seien Sie vorsichtig, falls Sie die Funktion deaktivieren möchten. Wenn die Distributed UMS-Funktion deaktiviert wird, aber mehrere UMS Server dieselbe Datenbank verwenden, wird keine Synchronisierung zwischen den UMS Servern durchgeführt.

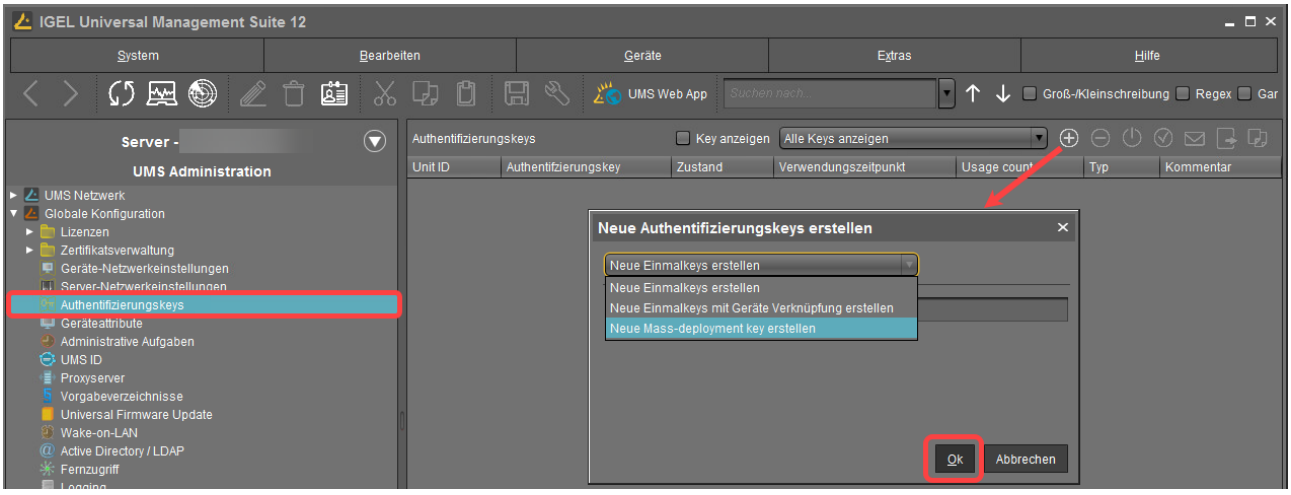
Authentifizierungskeys

Menüpfad: **UMS Administration > Globale Konfiguration > Authentifizierungskeys**

	Neue Authentifizierungskeys erzeugen
	Anmeldedaten löschen
	Anmeldedaten deaktivieren
	Anmeldedaten aktivieren
	Authentifizierungskeys mit E-Mail versenden
	Authentifizierungskeys exportieren (in den Formaten XML, HTML oder CSV)
	Authentifizierungskeys in die Zwischenablage kopieren

Wenn Sie einen Authentifizierungskey per E-Mail versenden, kann sich jeder, der die E-Mail lesen kann, beim IGEL Cloud Gateway anmelden. Es ist ratsam, das Senden per E-Mail mit einer Verknüpfung zu Unit IDs zu kombinieren.

Neue Authentifizierungskeys erstellen



Sie haben die folgenden Optionen:

- **Neue Einmalkeys erstellen**
  - **Anzahl**: Gewünschte Anzahl von Passwörtern, die erstellt werden sollen.
- **Neue Einmalkeys mit Geräte Verknüpfung erstellen**

- **Unit ID**
  - **Hinzufügen**: Fügt der Liste eine Unit ID hinzu, die im Textfeld eingegeben wurde.
  - **Selektieren**: Wählt die Unit ID eines Geräts aus dem UMS Strukturbaum aus.
  - **Importieren**: Liest eine CSV-Datei mit Unit IDs ein.
- **Neue Mass-deployment key erstellen**
  - **Zufälligen Mass-deployment key generieren**

    ☑ Ein zufälliges mehrfach verwendbares Passwort wird erzeugt. (Standard)

    ☐ Sie können das gewünschte Passwort selber eingeben.

    > Es ist nicht möglich, mehr als einen Authentifizierungskey mit demselben Passwort zu erstellen.

Geräteattribute für IGEL OS Geräte verwalten

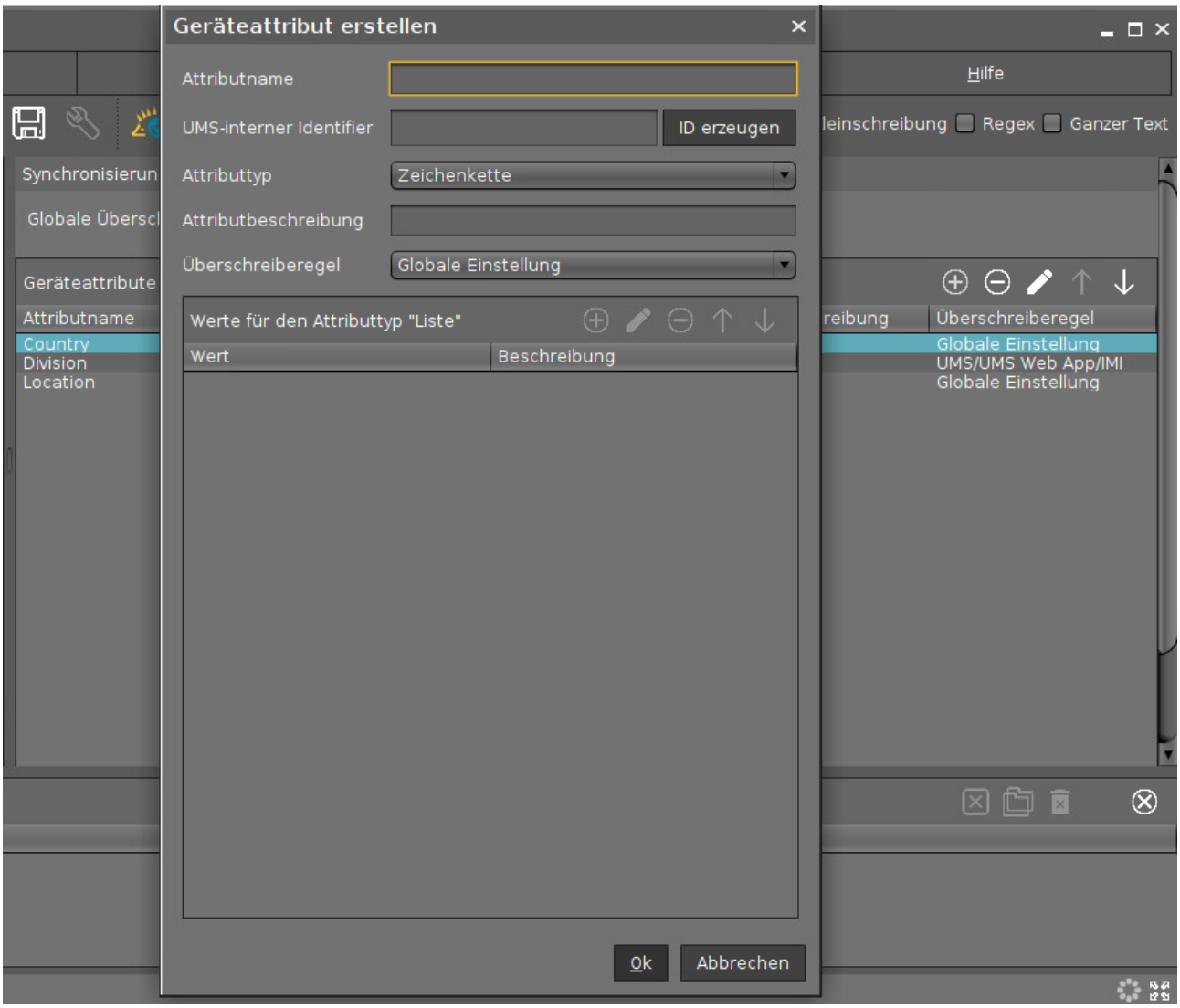
In diesem Bereich können Sie zusätzliche Attribute für IGEL OS-Geräte über die IGEL Universal Management Suite (UMS) einrichten. Diese Attribute werden zusammen mit den Standardgeräteattributen angezeigt, siehe Geräteinformationen in der IGEL UMS einsehen (see page 449). Sie können außerdem für die folgenden Funktionen verwendet werden:

- Suche in der UMS Konsole (see page 363) und in der Suche nach Geräten in der IGEL UMS Web App (see page 792)
- Views (see page 489)
- Vorgabeverzeichnisse (see page 643)

Bekannte Einschränkungen

Geräteattribute können nur innerhalb der UMS verwaltet werden; eine Export- oder Importfunktion ist nicht verfügbar.

Menüpfad: **UMS Administration > Globale Konfiguration > Geräteattribute**



▶ Klicken Sie ⊕, um ein neues Geräteattribut zu erstellen.

Globale Überschreiberegel

ⓘ Dieser Parameter ist relevant für Geräte mit IGEL OS 11.07 oder höher.

Legt die Standard-Überschreibregel für diejenigen Geräteattribute fest, deren Überschreiberegel auf **Globale Einstellung** gesetzt ist. Die Überschreiberegel legt fest, wie die Werte von Geräteattributen gesetzt und geändert werden.

Mögliche Optionen:

- **UMS/Web App/IMI**: Nur die UMS kann die Werte von Geräteattributen setzen und ändern. Dies gilt unabhängig davon, welche Schnittstelle für die Steuerung der UMS genutzt wird, d.h. UMS Konsole, UMS Web App oder IGEL Management Interface (IMI).

- **Geräte**: Nur die Geräte können die Werte von Geräteattributen setzen und ändern. Siehe auch Managing IGEL OS Devices by Device Specific Data - What Device Attributes Can Do for You (see page 172).
- **Alle**: Sowohl die UMS als auch die Geräte können die Werte von Geräteattributen setzen und ändern. Neue Werte überschreiben ältere Werte.

Attributname

Anzeigename des Attributs

UMS-interner Identifier

Dieser Identifikator ist für das Erstellen/Bearbeiten von Views oder das Bearbeiten von Suchen im Textmodus (text mode) erforderlich (siehe Wie erstelle ich eine neue View in der IGEL UMS? (see page 493)) sowie dafür, den Geräten das Setzen und Ändern von Attributewerten zu ermöglichen. Wenn Sie nicht vorhaben, eines dieser Features zu verwenden, können Sie dieses Feld leer lassen.

Sie können den Identifikator entweder automatisch generieren, indem Sie auf **ID erzeugen** klicken, oder ihn manuell angeben.

> Der **UMS-interne Identifier** muss mit Kleinbuchstaben beginnen. Nur die folgenden Zeichen sind zulässig: a-z, A-Z, 0-9.

Attributtyp

Datentyp des Attributs

Mögliche Werte:

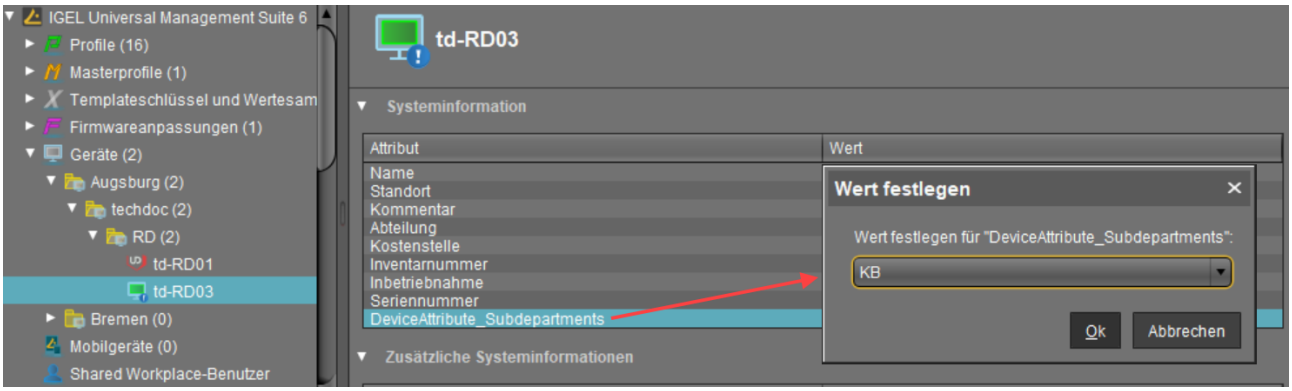
- **Zeichenkette**: Eine Folge von Buchstaben, Ziffern und Sonderzeichen wird erwartet.
- **Liste**: Eine Werteliste wird zur Auswahl vorgegeben. Diese legen Sie im Folgenden fest:
  Werte für den Attributtyp "Liste"
  - **Wert**: Name des vordefinierten Wertes
  - **Beschreibung**: Optionale Beschreibung des Wertes
- **Nummer**: Eine Zahlenwerteingabe wird erwartet.
- **Datum**: Eine Datumeingabe wird erwartet.

Attributbeschreibung

Optionale Beschreibung des Attributs

▶ Ändern Sie mit den Aufwärts- und Abwärts-Pfeilen die Reihenfolge der zusätzlichen Attribute.

▶ Unter **Systeminformationen** eines Geräts können Sie Werte für die Attribute festlegen.



Überschreiberegel

> ⓘ Dieser Parameter ist relevant für Geräte mit IGEL OS 11.07 oder höher.

Legt fest, wie der Wert dieses Geräteattributs gesetzt unf geändert werden kann.

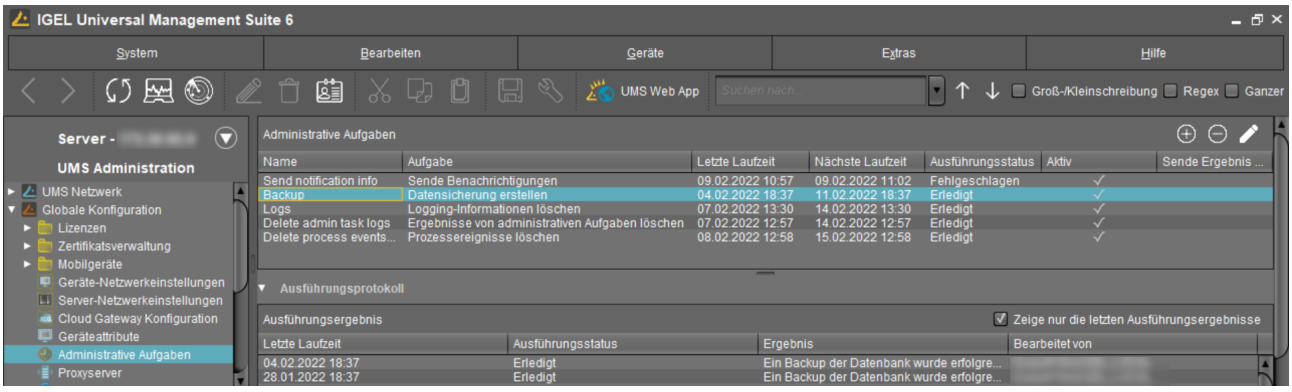
- **Globale Einstellung**: Die Globale Überschreiberegel ist für dieses Geräteattribut gültig.
- **UMS/Web App/IMI**: Nur die UMS kann die Werte von Geräteattributen setzen und ändern. Dies gilt unabhängig davon, welche Schnittstelle für die Steuerung der UMS genutzt wird, d.h. UMS Konsole, UMS Web App oder IGEL Management Interface (IMI).
- **Geräte**: Nur die Geräte können die Werte von Geräteattributen setzen und ändern. Siehe auch Managing IGEL OS Devices by Device Specific Data - What Device Attributes Can Do for You (see page 172).
- **Alle**: Sowohl die UMS als auch die Geräte können die Werte von Geräteattributen setzen und ändern. Neue Werte überschreiben ältere Werte.

Administrative Aufgaben - Zeitlich geplante Aktionen für die IGEL UMS konfigurieren

Sie können administrative Aufgaben für die IGEL Universal Management Suite (UMS) definieren. Eine Aufgabe besteht darin, eine Aktion automatisch zu einer definierten Zeit durchzuführen. Beispiele für solche Aktionen sind das Erstellen eines Datenbank-Backups (nur für Embedded-Datenbanken) oder das Entfernen unbenutzter Firmwaredateien. Aufgaben können in Intervallen oder an bestimmten Wochentagen wiederholt werden.

Um Probleme mit der Leistung der UMS und der Wiederherstellung von Backups zu vermeiden, wird dringend empfohlen, administrative Aufgaben zur automatischen Löschung von Protokollen – Logging-Informationen, Ergebnissen von Aufgaben, Ergebnissen von administrativen Aufgaben, Prozessereignissen, Verlauf der Assetinformationen – zu verwenden.
Einzelheiten finden Sie unter Leistungsoptimierungen (see page 294) und IGEL UMS Maintenance Tasks (see page 296).

Menüpfad: **UMS Administration > Globale Konfiguration > Administrative Aufgaben**



Neue administrative Aufgabe anlegen

So legen Sie eine neue administrative Aufgabe an:

1. Klicken Sie ⊕.
2. Legen Sie im Dialog **Eine neue administrative Aufgabe anlegen** die erforderlichen Einstellungen fest. Welche Einstellungen es gibt, hängt von der gewählten **Aktion** ab. Die Einstellungen sind auf mehrere Seiten verteilt, zwischen denen Sie mit **Weiter** und **Zurück** wechseln können.
   Die folgenden Aktionen stehen zur Verfügung:
   - Datensicherung erstellen (see page 599)
   - Unbenutzte Firmwares entfernen (see page 602)
   - Logging-Informationen löschen (see page 605)
   - Ergebnisse von Aufgaben löschen (see page 609)
   - Ergebnisse von administrativen Aufgaben löschen (see page 612)

- Prozessereignisse löschen (see page 615)
- Geräte löschen (see page 618)
- View oder Advanced Search Ergebnisse via Mail exportieren (see page 621)
- View oder Advanced Search Ergebnisse im Dateisystem speichern (see page 624)
- Objekte zu den Geräten von Views oder Geräte-Suchen zuordnen (see page 627)
- Entferne Objektzuordnungen von Geräten von Views oder Geräte-Suche (see page 630)
- Verlauf der Assetinformationen löschen (see page 633)
- Sende Benachrichtigungen via E-Mail (see page 636)

3. Klicken Sie **Fertig**.
   Die Aufgabe ist definiert und wird im Inhaltsbereich angezeigt. Der **Ausführungsstatus** zeigt an, ob die administrative Aufgabe erfolgreich ausgeführt wurde oder nicht.

Datensicherung erstellen

Sie können ein geplantes Backup der Datenbank als administrative Aufgabe definieren.

Menüpfad: **UMS Administration > Administrative Aufgaben >** Dialog "**Eine neue administrative Aufgabe anlegen**" **> Aktion** "**Datensicherung erstellen**"

Allgemein

Name

Name für die Aufgabe.

Aktion

▶ Wählen Sie **Datensicherung erstellen**.

Beschreibung
Optionale Beschreibung der Aufgabe.

Sende Ergebnis via Mail

☑ Das Ergebnis der Aufgabe wird per E-Mail an die festgelegten Empfänger gesendet.

Die folgenden zwei Optionen sind aktiv, falls **Sende Ergebnis via Mail** aktiviert ist:

An Hauptempfänger senden (nicht definiert)

☑ Die E-Mail wird an die unter **E-Mail-Einstellungen > E-Mail-Empfänger** definierte E-Mail-Adresse gesendet.
Weitere Informationen finden Sie unter E-Mail-Einstellungen (see page 664).

E-Mail-Empfänger
Weitere E-Mail-Adressen, an die die E-Mail gesendet wird. Wenn Sie mehrere Adressen eingeben, müssen Sie diese mit Semikolon ";" voneinander abtrennen.

Aktiv

☑ Die Aufgabe wird zum eingestellten Zeitpunkt ausgeführt. (Standard)

☐ Die Aufgabe wird nicht ausgeführt.

Konfiguration

Maximale Anzahl von Backups

Wenn im **Zielverzeichnis** die hier definierte Anzahl von Backup-Dateien erreicht ist, wird beim Anlegen eines neuen Backups die älteste Backup-Datei gelöscht. Bei "0" ist die Anzahl von Backup-Dateien unbegrenzt.

Zielverzeichnis für das erstellte Backup

Lokaler Verzeichnispfad auf dem UMS Server, in dem die Backup-Dateien gespeichert werden.

> Stellen Sie sicher, dass das Zielverzeichnis ein gültiger lokaler Verzeichnispfad auf dem UMS Server ist. Der UMS Server kann sich auf einem anderen Rechner befinden als die UMS Konsole.

Datensicherungskomponenten

Wählen Sie mindestens eine der folgenden Komponenten:

- **Datenbank (nur Embedded)**
- **Konfigurationen**
- **Dateien (nur Embedded)**

Serverzuordnung

> Die Seite "**Serverzuordnung**" wird nur bei der Verwendung der High-Availability- oder Distributed UMS (see page 246)-Umgebung angezeigt.

Zuordnungstyp

Mögliche Optionen:

- **Ein Server (zufällige Auswahl)**: Der Server für diese Aufgabe wird automatisch aus den unter **Zugeordnete Server** aufgelisteten Servern ausgewählt.
- **Ein Server (direkte Zuordnung)**: Sie können einen bestimmten Server für diese Aufgabe auswählen. Die verfügbaren Server sind unter **Zugeordnete Server** aufgelistet.
- **Alle Server**: Die Aufgabe wird von allen Servern durchgeführt.

Zugeordnete Server

Liste von Servern, die für diese Aufgabe verfügbar sind.

Zeitplan

Start
Zeitpunkt, an dem die Aufgabe ausgeführt wird.

Aufgabe startet alle [Anzahl Zeiteinheiten]

☑ Die Aufgabe wird im eingestellten Zeitintervall wiederholt.

☐ Die Aufgabe wird nicht im eingestellten Zeitintervall wiederholt.

Wochentage
Die Aufgabe wird an den aktivierten Wochentagen zum unter **Start** definierten Zeitpunkt ausgeführt.

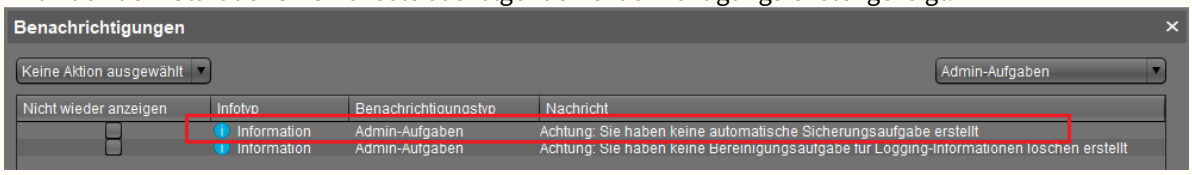
Monatlich
Die Aufgabe wird monatlich zum unter **Start** angegebenen Zeitpunkt ausgeführt.

Feiertage ausschließen
Die Aufgabe wird nicht ausgeführt an den Tagen, die in den über ... ausgewählten Feiertagslisten aufgelistet sind. Weitere Informationen zu den Feiertagslisten finden Sie in der Menüleiste unter **Extras > Geplante Aufgaben**, siehe Menüleiste der IGEL UMS Konsole (see page 343).

Ende
Zeitpunkt, ab dem die Aufgabe nicht mehr wiederholt wird.

Benachrichtigungen für Admin-Aufgaben

Falls Sie keine administrative Aufgabe für die Erstellung einer Datensicherung (see page 599) angelegt haben, wird nach dem Start der UMS Konsole das folgende Benachrichtigungsfenster gezeigt:



Diese Benachrichtigung können nur Benutzer mit den Leserechten für administrative Aufgaben sehen. Die Rechte können unter **Bearbeiten > Berechtigungen** definiert werden.
Anzeigeeinstellungen können unter **Extras > Einstellungen > Benachrichtigungen** angepasst werden.
Benachrichtigungen sind unter **Hilfe > Benachrichtigungen** zu finden.

Unbenutzte Firmwares entfernen

Sie können das Entfernen unbenutzter Firmware als administrative Aufgabe definieren. Die Löschung hilft bei der Leistungsoptimierung, siehe Performance Optimizations in IGEL UMS (see page 294).

> ⓘ Die erste Firmware, die in Ihrer UMS-Installation registriert wurde, kann nicht entfernt werden.

Menüpfad: **UMS Administration > Administrative Aufgaben >** Dialog **Eine neue administrative Aufgabe anlegen > Aktion "Unbenutzte Firmwares entfernen"**

Allgemein

Name

Name für die Aufgabe.

Aktion

▶ Wählen Sie **Unbenutzte Firmwares entfernen**.

Beschreibung
Optionale Beschreibung der Aufgabe.

Sende Ergebnis via Mail

☑ Das Ergebnis der Aufgabe wird per E-Mail an die festgelegten Empfänger gesendet.

Die folgenden zwei Optionen sind aktiv, falls **Sende Ergebnis via Mail** aktiviert ist:

An Hauptempfänger senden (nicht definiert)

☑ Die E-Mail wird an die unter **E-Mail-Einstellungen > E-Mail-Empfänger** definierte E-Mail-Adresse gesendet. Weitere Informationen finden Sie unter E-Mail-Einstellungen (see page 664).

E-Mail-Empfänger
Weitere E-Mail-Adressen, an die die E-Mail gesendet wird. Wenn Sie mehrere Adressen eingeben, müssen Sie diese mit Semikolon ";" voneinander abtrennen.

Aktiv

☑ Die Aufgabe wird zum eingestellten Zeitpunkt ausgeführt. (Standard)

☐ Die Aufgabe wird nicht ausgeführt.

Serverzuordnung

> ⓘ Die Seite "**Serverzuordnung**" wird nur bei der Verwendung der High-Availability- oder Distributed UMS (see page 246)-Umgebung angezeigt.

Zuordnungstyp

Mögliche Optionen:

- **Ein Server (zufällige Auswahl)**: Der Server für diese Aufgabe wird automatisch aus den unter **Zugeordnete Server** aufgelisteten Servern ausgewählt.
- **Ein Server (direkte Zuordnung)**: Sie können einen bestimmten Server für diese Aufgabe auswählen. Die verfügbaren Server sind unter **Zugeordnete Server** aufgelistet.
- **Alle Server**: Die Aufgabe wird von allen Servern durchgeführt.

Zugeordnete Server

Liste von Servern, die für diese Aufgabe verfügbar sind.

Zeitplan

Start
Zeitpunkt, an dem die Aufgabe ausgeführt wird.

Aufgabe startet alle [Anzahl Zeiteinheiten]

☑ Die Aufgabe wird im eingestellten Zeitintervall wiederholt.

☐ Die Aufgabe wird nicht im eingestellten Zeitintervall wiederholt.

Wochentage
Die Aufgabe wird an den aktivierten Wochentagen zum unter **Start** definierten Zeitpunkt ausgeführt.

Monatlich
Die Aufgabe wird monatlich zum unter **Start** angegebenen Zeitpunkt ausgeführt.

Feiertage ausschließen
Die Aufgabe wird nicht ausgeführt an den Tagen, die in den über ... ausgewählten Feiertagslisten aufgelistet sind. Weitere Informationen zu den Feiertagslisten finden Sie in der Menüleiste unter **Extras > Geplante Aufgaben**, siehe Menüleiste der IGEL UMS Konsole (see page 343).

Ende
Zeitpunkt, ab dem die Aufgabe nicht mehr wiederholt wird.

Logging-Informationen löschen

Sie können das Löschen von Nachrichten- und Ereignis-Logs der UMS als administrative Aufgabe definieren. Die Löschung hilft bei der Leistungsoptimierung, siehe Performance Optimizations in IGEL UMS (see page 294).

> ⓘ Die Protokolle für Sicheren Spiegeln (see page 486) sowie Leistungsprotokolle (see page 662) werden durch diese administrative Aufgabe nicht gelöscht.

Menüpfad: **UMS Administration > Administrative Aufgaben >** Dialog "**Eine neue administrative Aufgabe anlegen**" **> Aktion** "**Logging-Informationen löschen**"

Allgemein

Name

Name für die Aufgabe.

Aktion

▶ Wählen Sie **Logging-Informationen löschen**.

Beschreibung
Optionale Beschreibung der Aufgabe.

Sende Ergebnis via Mail

☑ Das Ergebnis der Aufgabe wird per E-Mail an die festgelegten Empfänger gesendet.

Die folgenden zwei Optionen sind aktiv, falls **Sende Ergebnis via Mail** aktiviert ist:

An Hauptempfänger senden (nicht definiert)

☑ Die E-Mail wird an die unter **E-Mail-Einstellungen > E-Mail-Empfänger** definierte E-Mail-Adresse gesendet. Weitere Informationen finden Sie unter E-Mail-Einstellungen (see page 664).

E-Mail-Empfänger
Weitere E-Mail-Adressen, an die die E-Mail gesendet wird. Wenn Sie mehrere Adressen eingeben, müssen Sie diese mit Semikolon ";" voneinander abtrennen.

Aktiv

☑ Die Aufgabe wird zum eingestellten Zeitpunkt ausgeführt. (Standard)

☐ Die Aufgabe wird nicht ausgeführt.

Konfiguration

Verzeichnis für exportierte Dateien

Lokaler Verzeichnispfad auf dem UMS Server, in dem die Backup-Dateien gespeichert werden. Wenn Sie das Feld leer lassen, wird das Verzeichnis `\rmguiserver\temp` verwendet. Der Dateinamen werden wie folgt gebildet: `Igel_log_events_.xml`, `Igel_log_messages_.xml.`

> Stellen Sie sicher, dass das Zielverzeichnis ein gültiger lokaler Verzeichnispfad auf dem UMS Server ist. Der UMS Server kann sich auf einem anderen Rechner befinden als die UMS Konsole. Wenn Sie kein Verzeichnis angeben, werden die Daten automatisch in folgendes Verzeichnis exportiert: `C:\Program Files\IGEL\RemoteManager\rmguiserver\temp`

Die folgenden Löscheinstellungen legen fest, welche Daten von der administrativen Aufgabe **Logging-Informationen löschen** gelöscht werden. Die Löscheinstellungen werden somit erst dann wirksam, wenn diese administrative Aufgabe ausgeführt wird.

Löscheinstellungen der Log-Nachrichten

- **Behalte nicht mehr als [Anzahl] Nachrichten**: Bei Ausführung dieser administrativen Aufgabe werden so viele der ältesten Protokolleinträge gelöscht, dass die hier eingestellte Anzahl von Protokolleinträgen erhalten bleibt. (Standard: 10 000)
  Beispiel: In der UMS seien 100 Protokolleinträge gespeichert. In der administrativen Aufgabe wird **Behalte nicht mehr als 10 Nachrichten** eingestellt. Beim Durchführen der administrativen Aufgabe werden die 90 ältesten Protokolleinträge gelöscht, während die 10 jüngsten Protokolleinträge erhalten bleiben.
- **Lösche Nachrichten, die älter sind als [Anzahl] Tage**: Protokolleinträge, die älter sind als die hier eingestellte Anzahl von Tagen, werden gelöscht. (Standard: 5)

Löscheinstellungen der Log-Ereignisse

- **Behalte nicht mehr als [Anzahl] Ereignisse**: Es werden so viele der ältesten Ereignisprotokolleinträge gelöscht, dass die hier eingestellte Anzahl von Ereignisprotokolleinträgen erhalten bleibt. (Standard: 10 000)
  Beispiel: In der UMS seien 100 Ereignisprotokolleinträge gespeichert. In der administrativen Aufgabe wird **Behalte nicht mehr als 10 Ereignisse** eingestellt. Beim Durchführen der administrativen Aufgabe werden die 90 ältesten Ereignisprotokolleinträge gelöscht, während die 10 jüngsten Ereignisprotokolleinträge erhalten bleiben.
- **Lösche Ereignisse, die älter sind als [Anzahl] Tage**: Ereignisprotokolleinträge, die älter sind als die hier eingestellte Anzahl von Tagen, werden gelöscht. (Standard: 5)

Serverzuordnung

> Die Seite "**Serverzuordnung**" wird nur bei der Verwendung der High-Availability- oder Distributed UMS (see page 246)-Umgebung angezeigt.

Zuordnungstyp

Mögliche Optionen:

- **Ein Server (zufällige Auswahl)**: Der Server für diese Aufgabe wird automatisch aus den unter **Zugeordnete Server** aufgelisteten Servern ausgewählt.
- **Ein Server (direkte Zuordnung)**: Sie können einen bestimmten Server für diese Aufgabe auswählen. Die verfügbaren Server sind unter **Zugeordnete Server** aufgelistet.
- **Alle Server**: Die Aufgabe wird von allen Servern durchgeführt.

Zugeordnete Server

Liste von Servern, die für diese Aufgabe verfügbar sind.

Zeitplan

Start
Zeitpunkt, an dem die Aufgabe ausgeführt wird.

Aufgabe startet alle [Anzahl Zeiteinheiten]

☑ Die Aufgabe wird im eingestellten Zeitintervall wiederholt.

☐ Die Aufgabe wird nicht im eingestellten Zeitintervall wiederholt.

Wochentage
Die Aufgabe wird an den aktivierten Wochentagen zum unter **Start** definierten Zeitpunkt ausgeführt.

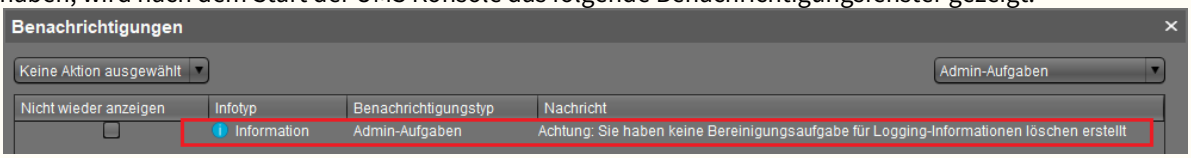
Monatlich
Die Aufgabe wird monatlich zum unter **Start** angegebenen Zeitpunkt ausgeführt.

Feiertage ausschließen
Die Aufgabe wird nicht ausgeführt an den Tagen, die in den über ... ausgewählten Feiertagslisten aufgelistet sind. Weitere Informationen zu den Feiertagslisten finden Sie in der Menüleiste unter **Extras > Geplante Aufgaben**, siehe Menüleiste der IGEL UMS Konsole (see page 343).

Ende
Zeitpunkt, ab dem die Aufgabe nicht mehr wiederholt wird.

Benachrichtigungen für Admin-Aufgaben

Falls Sie keine administrative Aufgabe für das Löschen von Logging-Informationen (see page 605) angelegt haben, wird nach dem Start der UMS Konsole das folgende Benachrichtigungsfenster gezeigt:



Diese Benachrichtigung können nur Benutzer mit den Leserechten für administrative Aufgaben sehen. Die Rechte können unter **Bearbeiten > Berechtigungen** definiert werden.
Anzeigeeinstellungen können unter **Extras > Einstellungen > Benachrichtigungen** angepasst werden.
Benachrichtigungen sind unter **Hilfe > Benachrichtigungen** zu finden.

Ergebnisse von Aufgaben löschen

Sie können das Löschen der Ergebnisse von Aufgaben als administrative Aufgabe definieren. Die Löschung hilft bei der Leistungsoptimierung, siehe Performance Optimizations in IGEL UMS (see page 294).

Menüpfad: **UMS Administration > Administrative Aufgaben >** Dialog "**Eine neue administrative Aufgabe anlegen**" **> Aktion** "**Ergebnisse von Aufgaben löschen**"

Allgemein

Name

Name für die Aufgabe.

Aktion

▶ Wählen Sie **Ergebnisse von Aufgaben löschen**.

Beschreibung
Optionale Beschreibung der Aufgabe.

Sende Ergebnis via Mail

☑ Das Ergebnis der Aufgabe wird per E-Mail an die festgelegten Empfänger gesendet.

Die folgenden zwei Optionen sind aktiv, falls **Sende Ergebnis via Mail** aktiviert ist:

An Hauptempfänger senden (nicht definiert)

☑ Die E-Mail wird an die unter **E-Mail-Einstellungen > E-Mail-Empfänger** definierte E-Mail-Adresse gesendet.
Weitere Informationen finden Sie unter E-Mail-Einstellungen (see page 664).

E-Mail-Empfänger
Weitere E-Mail-Adressen, an die die E-Mail gesendet wird. Wenn Sie mehrere Adressen eingeben, müssen Sie diese mit Semikolon ";" voneinander abtrennen.

Aktiv

☑ Die Aufgabe wird zum eingestellten Zeitpunkt ausgeführt. (Standard)

☐ Die Aufgabe wird nicht ausgeführt.

Konfiguration

Verzeichnis für exportierte Dateien

Verzeichnis auf dem UMS Server, in dem die Logging-Daten gesichert werden sollen, bevor sie aus der UMS Datenbank gelöscht werden. Die Daten werden erst dann aus der Datenbank gelöscht, wenn die Sicherung erfolgreich war. Wenn Sie das Feld leer lassen, wird das Verzeichnis `\rmguiserver\temp` verwendet. Der Dateiname für die Logging-Daten wird wie folgt gebildet: `Igel_deleted_job_exec_.csv` .

Löscheinstellungen

Hier können Sie festlegen, nach welchen Kriterien Protokolle zu Aufgaben gelöscht werden.

- **Behalte nicht mehr als [Anzahl] Ausführungen pro Aufgabe**: Jede Aufgabe hat Ausführungen. Jede Ausführung kann Tausende von Ergebnissen haben. Diese Aufgabe löscht alle Ausführungen und deren Ergebnisse bis auf die angegebene Zahl von den neusten Ausführungen. (Standard: 10)
- **Lösche Ereignisse, die älter sind als [Anzahl] Tage**: Protokolle, die älter sind als die hier eingestellte Anzahl von Tagen, werden gelöscht. (Standard: 5)

Serverzuordnung

> Die Seite "**Serverzuordnung**" wird nur bei der Verwendung der High-Availability- oder Distributed UMS (see page 246)-Umgebung angezeigt.

Zuordnungstyp

Mögliche Optionen:

- **Ein Server (zufällige Auswahl)**: Der Server für diese Aufgabe wird automatisch aus den unter **Zugeordnete Server** aufgelisteten Servern ausgewählt.
- **Ein Server (direkte Zuordnung)**: Sie können einen bestimmten Server für diese Aufgabe auswählen. Die verfügbaren Server sind unter **Zugeordnete Server** aufgelistet.
- **Alle Server**: Die Aufgabe wird von allen Servern durchgeführt.

Zugeordnete Server

Liste von Servern, die für diese Aufgabe verfügbar sind.

Zeitplan

Start
Zeitpunkt, an dem die Aufgabe ausgeführt wird.

Aufgabe startet alle [Anzahl Zeiteinheiten]

☑ Die Aufgabe wird im eingestellten Zeitintervall wiederholt.

☐ Die Aufgabe wird nicht im eingestellten Zeitintervall wiederholt.

Wochentage
Die Aufgabe wird an den aktivierten Wochentagen zum unter **Start** definierten Zeitpunkt ausgeführt.

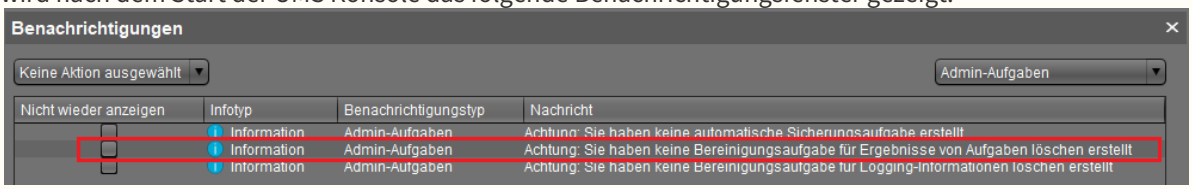
Monatlich
Die Aufgabe wird monatlich zum unter **Start** angegebenen Zeitpunkt ausgeführt.

Feiertage ausschließen
Die Aufgabe wird nicht ausgeführt an den Tagen, die in den über ... ausgewählten Feiertagslisten aufgelistet sind. Weitere Informationen zu den Feiertagslisten finden Sie in der Menüleiste unter **Extras > Geplante Aufgaben**, siehe Menüleiste der IGEL UMS Konsole (see page 343).

Ende
Zeitpunkt, ab dem die Aufgabe nicht mehr wiederholt wird.

Benachrichtigungen für Admin-Aufgaben

Falls Sie keine administrative Aufgabe "Ergebnisse von Aufgaben löschen (see page 609)" angelegt haben, wird nach dem Start der UMS Konsole das folgende Benachrichtigungsfenster gezeigt:



Diese Benachrichtigung können nur Benutzer mit den Leserechten für administrative Aufgaben sehen. Die Rechte können unter **Bearbeiten > Berechtigungen** definiert werden.
Anzeigeeinstellungen können unter **Extras > Einstellungen > Benachrichtigungen** angepasst werden.
Benachrichtigungen sind unter **Hilfe > Benachrichtigungen** zu finden.

Ergebnisse von administrativen Aufgaben löschen

Sie können das Löschen der Ergebnisse von Administrativen Aufgaben (see page 597) als administrative Aufgabe definieren. Die Löschung hilft bei der Leistungsoptimierung, siehe Performance Optimizations in IGEL UMS (see page 294).

Menüpfad: **UMS Administration > Administrative Aufgaben >** Dialog **Eine neue administrative Aufgabe anlegen > Aktion "Ergebnisse von administrativen Aufgaben löschen"**

Allgemein

Name

Name für die Aufgabe.

Aktion

▶ Wählen Sie **Ergebnisse von administrativen Aufgaben löschen**.

Beschreibung
Optionale Beschreibung der Aufgabe.

Sende Ergebnis via Mail

☑ Das Ergebnis der Aufgabe wird per E-Mail an die festgelegten Empfänger gesendet.

Die folgenden zwei Optionen sind aktiv, falls **Sende Ergebnis via Mail** aktiviert ist:

An Hauptempfänger senden (nicht definiert)

☑ Die E-Mail wird an die unter **E-Mail-Einstellungen > E-Mail-Empfänger** definierte E-Mail-Adresse gesendet. Weitere Informationen finden Sie unter E-Mail-Einstellungen (see page 664).

E-Mail-Empfänger
Weitere E-Mail-Adressen, an die die E-Mail gesendet wird. Wenn Sie mehrere Adressen eingeben, müssen Sie diese mit Semikolon ";" voneinander abtrennen.

Aktiv

☑ Die Aufgabe wird zum eingestellten Zeitpunkt ausgeführt. (Standard)

☐ Die Aufgabe wird nicht ausgeführt.

Konfiguration

Verzeichnis für exportierte Dateien

Verzeichnis auf dem UMS Server, in dem die Logging-Daten gesichert werden sollen. Die Daten werden erst dann aus der Datenbank gelöscht, wenn die Sicherung erfolgreich war. Wenn Sie das Feld leer lassen, wird das Verzeichnis `\rmguiserver\temp` verwendet. Der Dateiname für die Logging-Daten wird wie folgt gebildet: `Igel_deleted_job_exec_.csv`.

Behalte nicht mehr als [Anzahl] Ausführungen pro administrative Aufgabe

Jede administrative Aufgabe hat Ausführungen. Jede Ausführung kann Tausende von Ergebnissen haben. Diese Aufgabe löscht alle Ausführungen und deren Ergebnisse bis auf die angegebene Zahl von den neusten Ausführungen. (Standard: 10)

Lösche Ereignisse, die älter sind als [Anzahl] Tage

Ereignissprotokolleinträge, die älter sind als die hier eingestellte Anzahl von Tagen, werden gelöscht. (Standard: 5)

Serverzuordnung

> Die Seite "**Serverzuordnung**" wird nur bei der Verwendung der High-Availability- oder Distributed UMS (see page 246)-Umgebung angezeigt.

Zuordnungstyp

Mögliche Optionen:

- **Ein Server (zufällige Auswahl)**: Der Server für diese Aufgabe wird automatisch aus den unter **Zugeordnete Server** aufgelisteten Servern ausgewählt.
- **Ein Server (direkte Zuordnung)**: Sie können einen bestimmten Server für diese Aufgabe auswählen. Die verfügbaren Server sind unter **Zugeordnete Server** aufgelistet.
- **Alle Server**: Die Aufgabe wird von allen Servern durchgeführt.

Zugeordnete Server

Liste von Servern, die für diese Aufgabe verfügbar sind.

Zeitplan

Start
Zeitpunkt, an dem die Aufgabe ausgeführt wird.

Aufgabe startet alle [Anzahl Zeiteinheiten]

☑ Die Aufgabe wird im eingestellten Zeitintervall wiederholt.

☐ Die Aufgabe wird nicht im eingestellten Zeitintervall wiederholt.

Wochentage
Die Aufgabe wird an den aktivierten Wochentagen zum unter **Start** definierten Zeitpunkt ausgeführt.

Monatlich
Die Aufgabe wird monatlich zum unter **Start** angegebenen Zeitpunkt ausgeführt.

Feiertage ausschließen
Die Aufgabe wird nicht ausgeführt an den Tagen, die in den über  ausgewählten Feiertagslisten aufgelistet sind. Weitere Informationen zu den Feiertagslisten finden Sie in der Menüleiste unter **Extras > Geplante Aufgaben**, siehe Menüleiste der IGEL UMS Konsole (see page 343).

Ende
Zeitpunkt, ab dem die Aufgabe nicht mehr wiederholt wird.

Prozessereignisse löschen

Sie können das Löschen von Prozessereignissen als administrative Aufgabe definieren. Die Löschung hilft bei der Leistungsoptimierung, siehe Performance Optimizations in IGEL UMS (see page 294).

Menüpfad: **UMS Administration > Administrative Aufgaben >** Dialog **Eine neue administrative Aufgabe anlegen > Aktion "Prozessereignisse löschen"**

Allgemein

Name

Name für die Aufgabe.

Aktion

▶ Wählen Sie **Prozessereignisse löschen**.

Beschreibung
Optionale Beschreibung der Aufgabe.

Sende Ergebnis via Mail

☑ Das Ergebnis der Aufgabe wird per E-Mail an die festgelegten Empfänger gesendet.

Die folgenden zwei Optionen sind aktiv, falls **Sende Ergebnis via Mail** aktiviert ist:

An Hauptempfänger senden (nicht definiert)

☑ Die E-Mail wird an die unter **E-Mail-Einstellungen > E-Mail-Empfänger** definierte E-Mail-Adresse gesendet.
Weitere Informationen finden Sie unter E-Mail-Einstellungen (see page 664).

E-Mail-Empfänger
Weitere E-Mail-Adressen, an die die E-Mail gesendet wird. Wenn Sie mehrere Adressen eingeben, müssen Sie diese mit Semikolon ";" voneinander abtrennen.

Aktiv

☑ Die Aufgabe wird zum eingestellten Zeitpunkt ausgeführt. (Standard)

☐ Die Aufgabe wird nicht ausgeführt.

Konfiguration

Verzeichnis für exportierte Dateien

Verzeichnis auf dem UMS Server, in dem die Logging-Daten gesichert werden sollen, bevor sie aus der UMS Datenbank gelöscht werden. Die Daten werden erst dann aus der Datenbank gelöscht, wenn die Sicherung erfolgreich war. Wenn Sie das Feld leer lassen, wird das Verzeichnis `\rmguiserver\temp` verwendet. Der Dateiname für die Logging-Daten wird wie folgt gebildet: `Igel_deleted_job_exec_.csv`.

Behalte nicht mehr als [Anzahl] Prozessereignisse

Bei Ausführung dieser administrativen Aufgabe werden so viele der ältesten Protokolleinträge gelöscht, dass die hier eingestellte Anzahl von Protokolleinträgen erhalten bleibt. (Standard: 1 000)
Beispiel: In der UMS seien 100 Protokolleinträge gespeichert. In der administrativen Aufgabe wird **Behalte nicht mehr als 10 Prozessereignisse** eingestellt. Beim Durchführen der administrativen Aufgabe werden die 90 ältesten Protokolleinträge gelöscht, während die 10 jüngsten Protokolleinträge erhalten bleiben.

Lösche Ereignisse, die älter sind als [Anzahl] Tage

Ereignissprotokolleinträge, die älter sind als die hier eingestellte Anzahl von Tagen, werden gelöscht. (Standard: 5)

Serverzuordnung

> Die Seite "**Serverzuordnung**" wird nur bei der Verwendung der High-Availability- oder Distributed UMS (see page 246)-Umgebung angezeigt.

Zuordnungstyp

Mögliche Optionen:

- **Ein Server (zufällige Auswahl)**: Der Server für diese Aufgabe wird automatisch aus den unter **Zugeordnete Server** aufgelisteten Servern ausgewählt.
- **Ein Server (direkte Zuordnung)**: Sie können einen bestimmten Server für diese Aufgabe auswählen. Die verfügbaren Server sind unter **Zugeordnete Server** aufgelistet.
- **Alle Server**: Die Aufgabe wird von allen Servern durchgeführt.

Zugeordnete Server

Liste von Servern, die für diese Aufgabe verfügbar sind.

Zeitplan

Start
Zeitpunkt, an dem die Aufgabe ausgeführt wird.

Aufgabe startet alle [Anzahl Zeiteinheiten]

☑ Die Aufgabe wird im eingestellten Zeitintervall wiederholt.

☐ Die Aufgabe wird nicht im eingestellten Zeitintervall wiederholt.

Wochentage
Die Aufgabe wird an den aktivierten Wochentagen zum unter **Start** definierten Zeitpunkt ausgeführt.

Monatlich
Die Aufgabe wird monatlich zum unter **Start** angegebenen Zeitpunkt ausgeführt.

Feiertage ausschließen
Die Aufgabe wird nicht ausgeführt an den Tagen, die in den über ... ausgewählten Feiertagslisten aufgelistet sind. Weitere Informationen zu den Feiertagslisten finden Sie in der Menüleiste unter **Extras > Geplante Aufgaben**, siehe Menüleiste der IGEL UMS Konsole (see page 343).

Ende
Zeitpunkt, ab dem die Aufgabe nicht mehr wiederholt wird.

Geräte löschen

Sie können eine administrative Aufgabe definieren, durch die bestimmte Geräte aus der UMS Datenbank gelöscht werden. Welche Geräte gelöscht werden, ist durch die Kriterien einer View oder einer Advanced Search definiert. Zum Beispiel, Sie können alle Geräte herausfiltern, die länger als ein Jahr nicht mehr gestartet wurden und dann eine administrative Aufgabe definieren um sie zu löschen.

Weitere Informationen über die Advanced Search in der UMS Web App finden Sie unter Suche nach Geräten in der IGEL UMS Web App (see page 792).

Menüpfad: **UMS Administration > Administrative Aufgaben >** Dialog **Eine neue administrative Aufgabe anlegen > Aktion "Geräte löschen"**

Allgemein

Name

Name für die Aufgabe.

Aktion

▶ Wählen Sie **Geräte löschen**.

Beschreibung
Optionale Beschreibung der Aufgabe.

Sende Ergebnis via Mail

☑ Das Ergebnis der Aufgabe wird per E-Mail an die festgelegten Empfänger gesendet.

Die folgenden zwei Optionen sind aktiv, falls **Sende Ergebnis via Mail** aktiviert ist:

An Hauptempfänger senden (nicht definiert)

☑ Die E-Mail wird an die unter **E-Mail-Einstellungen > E-Mail-Empfänger** definierte E-Mail-Adresse gesendet.
Weitere Informationen finden Sie unter E-Mail-Einstellungen (see page 664).

E-Mail-Empfänger
Weitere E-Mail-Adressen, an die die E-Mail gesendet wird. Wenn Sie mehrere Adressen eingeben, müssen Sie diese mit Semikolon ";" voneinander abtrennen.

Aktiv

☑ Die Aufgabe wird zum eingestellten Zeitpunkt ausgeführt. (Standard)

☐ Die Aufgabe wird nicht ausgeführt.

Konfiguration

Geräte folgender View / Advanced Search löschen

View / Advanced Search, die die Kriterien für das Löschen der Geräte festlegt. Die View / Advanced Search wird über die Schaltfläche ... ausgewählt.

View ID / Advanced Search ID

ID der ausgewählten View / Advanced Search.

Serverzuordnung

> ⓘ Die Seite "**Serverzuordnung**" wird nur bei der Verwendung der High-Availability- oder Distributed UMS (see page 246)-Umgebung angezeigt.

Zuordnungstyp

Mögliche Optionen:

- **Ein Server (zufällige Auswahl)**: Der Server für diese Aufgabe wird automatisch aus den unter **Zugeordnete Server** aufgelisteten Servern ausgewählt.
- **Ein Server (direkte Zuordnung)**: Sie können einen bestimmten Server für diese Aufgabe auswählen. Die verfügbaren Server sind unter **Zugeordnete Server** aufgelistet.
- **Alle Server**: Die Aufgabe wird von allen Servern durchgeführt.

Zugeordnete Server

Liste von Servern, die für diese Aufgabe verfügbar sind.

Zeitplan

Start
Zeitpunkt, an dem die Aufgabe ausgeführt wird.

Aufgabe startet alle [Anzahl Zeiteinheiten]

☑ Die Aufgabe wird im eingestellten Zeitintervall wiederholt.

☐ Die Aufgabe wird nicht im eingestellten Zeitintervall wiederholt.

Wochentage
Die Aufgabe wird an den aktivierten Wochentagen zum unter **Start** definierten Zeitpunkt ausgeführt.

Monatlich
Die Aufgabe wird monatlich zum unter **Start** angegebenen Zeitpunkt ausgeführt.

Feiertage ausschließen
Die Aufgabe wird nicht ausgeführt an den Tagen, die in den über ... ausgewählten Feiertagslisten aufgelistet sind. Weitere Informationen zu den Feiertagslisten finden Sie in der Menüleiste unter **Extras > Geplante Aufgaben**, siehe Menüleiste der IGEL UMS Konsole (see page 343).

Ende
Zeitpunkt, ab dem die Aufgabe nicht mehr wiederholt wird.

View oder Advanced Search Ergebnisse via Mail exportieren

Sie können eine administrative Aufgabe definieren, durch die die Ergebnisse einer View oder Advanced Search als E-Mail-Anhang exportiert werden. Weitere Informationen über die Advanced Search in der UMS Web App finden Sie unter Search for Devices in the IGEL UMS Web App.

> ⓘ Für das Versenden von E-Mails müssen die Mail-Einstellungen der UMS korrekt sein. Weitere Informationen finden Sie unter E-Mail-Einstellungen (see page 664).

Menüpfad: **UMS Administration > Administrative Aufgaben >** Dialog **Eine neue administrative Aufgabe anlegen >** Aktion **"View-Ergebnisse via Mail exportieren"**

Allgemein

Name

Name für die Aufgabe.

Aktion

▶ Wählen Sie **View-/Advanced Search-Ergebnisse via Mail exportieren**.

Beschreibung
Optionale Beschreibung der Aufgabe.

Sende Ergebnis via Mail

☑ Das Ergebnis der Aufgabe wird per E-Mail an die festgelegten Empfänger gesendet.

Die folgenden zwei Optionen sind aktiv, falls **Sende Ergebnis via Mail** aktiviert ist:

An Hauptempfänger senden (nicht definiert)

☑ Die E-Mail wird an die unter **E-Mail-Einstellungen > E-Mail-Empfänger** definierte E-Mail-Adresse gesendet. Weitere Informationen finden Sie unter E-Mail-Einstellungen (see page 664).

E-Mail-Empfänger
Weitere E-Mail-Adressen, an die die E-Mail gesendet wird. Wenn Sie mehrere Adressen eingeben, müssen Sie diese mit Semikolon ";" voneinander abtrennen.

Aktiv

☑ Die Aufgabe wird zum eingestellten Zeitpunkt ausgeführt. (Standard)

☐ Die Aufgabe wird nicht ausgeführt.

Konfiguration

View ID / Advanced Search ID

ID der ausgewählten View / Advanced Search. Die View / Advanced Search wird über die Schaltfläche … ausgewählt.

Konfiguration sichtbarer Spalten

Datenfelder, die in der E-Mail enthalten sein sollen.

View-/Advanced Search-Exportname

Benutzerdefinierter Name für die Exportdatei (optional). Datum und Uhrzeit werden automatisch hinzugefügt, abgetrennt durch einen Unterstrich. Beispiel: `CUSTOMNAME_2021-05-02_10-34.xml`

E-Mail-Empfänger

E-Mail-Adressen der Empfänger. Wenn Sie mehrere Adressen eingeben, müssen Sie diese mit Semikolon ";" voneinander abtrennen.

Exportformat

Datenformat, in dem die Ergebnisse als E-Mail-Anhang verschickt werden.
Mögliche Optionen:

- **XML**
- **HTML**
- **CSV**

Archiv erstellen

☑ Der E-Mail-Anhang wird als ZIP-Archiv komprimiert.

☐ Der E-Mail-Anhang behält sein Datenformat bei (XML, HTML oder CSV). (Standard)

Serverzuordnung

> ⓘ Die Seite "**Serverzuordnung**" wird nur bei der Verwendung der High-Availability- oder Distributed UMS (see page 246)-Umgebung angezeigt.

Zuordnungstyp

Mögliche Optionen:

- **Ein Server (zufällige Auswahl)**: Der Server für diese Aufgabe wird automatisch aus den unter **Zugeordnete Server** aufgelisteten Servern ausgewählt.
- **Ein Server (direkte Zuordnung)**: Sie können einen bestimmten Server für diese Aufgabe auswählen. Die verfügbaren Server sind unter **Zugeordnete Server** aufgelistet.
- **Alle Server**: Die Aufgabe wird von allen Servern durchgeführt.

Zugeordnete Server

Liste von Servern, die für diese Aufgabe verfügbar sind.

Zeitplan

Start
Zeitpunkt, an dem die Aufgabe ausgeführt wird.

Aufgabe startet alle [Anzahl Zeiteinheiten]

☑ Die Aufgabe wird im eingestellten Zeitintervall wiederholt.

☐ Die Aufgabe wird nicht im eingestellten Zeitintervall wiederholt.

Wochentage
Die Aufgabe wird an den aktivierten Wochentagen zum unter **Start** definierten Zeitpunkt ausgeführt.

Monatlich
Die Aufgabe wird monatlich zum unter **Start** angegebenen Zeitpunkt ausgeführt.

Feiertage ausschließen
Die Aufgabe wird nicht ausgeführt an den Tagen, die in den über  ausgewählten Feiertagslisten aufgelistet sind. Weitere Informationen zu den Feiertagslisten finden Sie in der Menüleiste unter **Extras > Geplante Aufgaben**, siehe Menüleiste der IGEL UMS Konsole (see page 343).

Ende
Zeitpunkt, ab dem die Aufgabe nicht mehr wiederholt wird.

View oder Advanced Search Ergebnisse im Dateisystem speichern

In der IGEL Universal Management Suite (UMS) können Sie eine administrative Aufgabe definieren, um die Ergebnisse einer in der UMS Konsole erstellten Ansicht oder die Ergebnisse einer in der UMS Web App erstellten Advanced Search zu speichern. Die Ergebnisse werden im Dateisystem des UMS-Servers gespeichert.

Allgemeine Informationen zu administrativen Aufgaben finden Sie unter Administrative Aufgaben - Zeitlich geplante Aktionen für die IGEL UMS konfigurieren (see page 597). Weitere Informationen über die Advanced Search in der UMS Web App finden Sie unter Search for Devices in the IGEL UMS Web App.

Menüpfad: **UMS Administration > Administrative Aufgaben >** Dialog "**Eine neue administrative Aufgabe anlegen**" **>** Aktion "**View-/Advanced Search-Ergebnisse im Dateisystem speichern**"

Allgemein

Name

Name für die Aufgabe.

Aktion

▶ Wählen Sie **View-/Advanced Search-Ergebnisse im Dateisystem speichern**.

Beschreibung
Optionale Beschreibung der Aufgabe.

Sende Ergebnis via Mail

☑ Das Ergebnis der Aufgabe wird per E-Mail an die festgelegten Empfänger gesendet.

Die folgenden zwei Optionen sind aktiv, falls **Sende Ergebnis via Mail** aktiviert ist:

An Hauptempfänger senden (nicht definiert)

☑ Die E-Mail wird an die unter **E-Mail-Einstellungen > E-Mail-Empfänger** definierte E-Mail-Adresse gesendet. Weitere Informationen finden Sie unter E-Mail-Einstellungen (see page 664).

E-Mail-Empfänger
Weitere E-Mail-Adressen, an die die E-Mail gesendet wird. Wenn Sie mehrere Adressen eingeben, müssen Sie diese mit Semikolon ";" voneinander abtrennen.

Aktiv

☑ Die Aufgabe wird zum eingestellten Zeitpunkt ausgeführt. (Standard)

☐ Die Aufgabe wird nicht ausgeführt.

Konfiguration

View ID / Advanced Search ID

ID der ausgewählten View / Advanced Search. Die View / Advanced Search wird über die Schaltfläche … ausgewählt.

Konfiguration sichtbarer Spalten

Datenfelder, die in der E-Mail enthalten sein sollen. Die Datenfelder werden über die Schaltfläche … ausgewählt. Mit dem Kontrollkästchen neben **Spaltenname** können Sie alle Datenfelder auf einmal auswählen.

View- / Advanced Search-Exportname

Benutzerdefinierter Name für die Exportdatei (optional). Datum und Uhrzeit werden automatisch hinzugefügt, abgetrennt durch einen Unterstrich. Beispiel: `CUSTOMNAME_2021-05-02_10-34.xml`

Zielverzeichnis für die Export-Dateien

Verzeichnis auf dem UMS Server, in dem die View-Ergebnisse gespeichert werden. Wenn nichts angegeben ist, wird das Standardverzeichnis verwendet. Das Zielverzeichnis wird unter dem Eingabefeld angezeigt. Beispiel: `C:\Program Files\IGEL\RemoteManager\rmguiserver\temp`

> ⓘ Ob ein Netzlaufwerkverzeichnis als Zielverzeichnis akzeptiert wird, hängt von der Konfiguration des Netzlaufwerks ab. Beispiel: Wenn für den Zugriff auf das Netzlaufwerkverzeichnis eine Authentifizierung erforderlich ist, schlägt die Ausführung der administrativen Aufgabe fehl.

Exportformat

Datenformat, in dem die Ergebnisse gespeichert werden.
Mögliche Optionen:

- **XML**
- **HTML**
- **CSV**

Archiv erstellen

☑ Die Datei wird als ZIP-Archiv komprimiert.

☐ Die Datei behält ihr Datenformat bei (XML, HTML oder CSV). (Standard)

Zeitplan

Start
Zeitpunkt, an dem die Aufgabe ausgeführt wird.

Aufgabe startet alle [Anzahl Zeiteinheiten]

☑ Die Aufgabe wird im eingestellten Zeitintervall wiederholt.

☐ Die Aufgabe wird nicht im eingestellten Zeitintervall wiederholt.

Wochentage
Die Aufgabe wird an den aktivierten Wochentagen zum unter **Start** definierten Zeitpunkt ausgeführt.

Monatlich
Die Aufgabe wird monatlich zum unter **Start** angegebenen Zeitpunkt ausgeführt.

Feiertage ausschließen
Die Aufgabe wird nicht ausgeführt an den Tagen, die in den über  ausgewählten Feiertagslisten aufgelistet sind. Weitere Informationen zu den Feiertagslisten finden Sie in der Menüleiste unter **Extras > Geplante Aufgaben**, siehe Menüleiste der IGEL UMS Konsole (see page 343).

Ende
Zeitpunkt, ab dem die Aufgabe nicht mehr wiederholt wird.

Objekte zu den Geräten von Views oder Geräte-Suchen zuordnen

Sie können den Geräten, die Sie über eine View oder Suche in der UMS Konsole oder über die Advanced Search in der UMS Web App gefiltert haben, Objekte zuweisen. Sie können diese Zuordnung regelmäßig über einen Zeitplan aktualisieren.

Weitere Informationen über die Advanced Search in der UMS Web App finden Sie unter Suche nach Geräten in der IGEL UMS Web App (see page 792).

Beachten Sie auch die Anleitung Einer View Objekte zuordnen (see page 517).

Menüpfad: **UMS Administration > Administrative Aufgaben >** Dialog **Eine neue administrative Aufgabe anlegen > Aktion "Objekte zu den Geräten von Views / Advanced Searches zuordnen"**

Allgemein

Name

Name für die Aufgabe.

Aktion

▶ Wählen Sie **Objekte zu den Geräten von Views / Advanced Searches zuordnen**.

Beschreibung
Optionale Beschreibung der Aufgabe.

Sende Ergebnis via Mail

☑ Das Ergebnis der Aufgabe wird per E-Mail an die festgelegten Empfänger gesendet.

Die folgenden zwei Optionen sind aktiv, falls **Sende Ergebnis via Mail** aktiviert ist:

An Hauptempfänger senden (nicht definiert)

☑ Die E-Mail wird an die unter **E-Mail-Einstellungen > E-Mail-Empfänger** definierte E-Mail-Adresse gesendet.
Weitere Informationen finden Sie unter E-Mail-Einstellungen (see page 664).

E-Mail-Empfänger
Weitere E-Mail-Adressen, an die die E-Mail gesendet wird. Wenn Sie mehrere Adressen eingeben, müssen Sie diese mit Semikolon ";" voneinander abtrennen.

Aktiv

☑ Die Aufgabe wird zum eingestellten Zeitpunkt ausgeführt. (Standard)

☐ Die Aufgabe wird nicht ausgeführt.

Views / Geräte-Suchen auswählen

▶ Wählen Sie eine View / Geräte-Suche / Advanced Search und klicken Sie auf  um sie zu der Liste hinzuzufügen, die einem oder mehreren Objekten zugewiesen werden soll.

Objekte auswählen

▶ Wählen Sie eine Objekte aus und klicken Sie auf  um sie zu der Liste hinzuzufügen, der Sie die View oder die Gerätesuche zuordnen möchten.

Objekte können sein:

- Profile
- Firmwareanpassungen
- Dateien
- Firmwareupdates.

Serverzuordnung

> ⓘ Die Seite "**Serverzuordnung**" wird nur bei der Verwendung der High-Availability- oder Distributed UMS (see page 246)-Umgebung angezeigt.

Zuordnungstyp

Mögliche Optionen:

- **Ein Server (zufällige Auswahl)**: Der Server für diese Aufgabe wird automatisch aus den unter **Zugeordnete Server** aufgelisteten Servern ausgewählt.
- **Ein Server (direkte Zuordnung)**: Sie können einen bestimmten Server für diese Aufgabe auswählen. Die verfügbaren Server sind unter **Zugeordnete Server** aufgelistet.
- **Alle Server**: Die Aufgabe wird von allen Servern durchgeführt.

Zugeordnete Server

Liste von Servern, die für diese Aufgabe verfügbar sind.

Zeitplan

Start
Zeitpunkt, an dem die Aufgabe ausgeführt wird.

Aufgabe startet alle [Anzahl Zeiteinheiten]

☑ Die Aufgabe wird im eingestellten Zeitintervall wiederholt.

☐ Die Aufgabe wird nicht im eingestellten Zeitintervall wiederholt.

Wochentage
Die Aufgabe wird an den aktivierten Wochentagen zum unter **Start** definierten Zeitpunkt ausgeführt.

Monatlich
Die Aufgabe wird monatlich zum unter **Start** angegebenen Zeitpunkt ausgeführt.

Feiertage ausschließen
Die Aufgabe wird nicht ausgeführt an den Tagen, die in den über  ausgewählten Feiertagslisten aufgelistet sind. Weitere Informationen zu den Feiertagslisten finden Sie in der Menüleiste unter **Extras > Geplante Aufgaben**, siehe Menüleiste der IGEL UMS Konsole (see page 343).

Ende
Zeitpunkt, ab dem die Aufgabe nicht mehr wiederholt wird.

Entferne Objektzuordnungen von Geräten von Views oder Geräte-Suche

In der IGEL Universal Management Suite (UMS) können Sie eine administrative Aufgabe erstellen, um zugewiesene Objekte von Geräten zu trennen, die Sie über eine View oder Suche in der UMS-Konsole oder über eine Advanced Search in der UMS Web App gefiltert haben. Sie können Objekte von den Geräten der View oder der Suche auch manuell entfernen, siehe Einer View Objekte zuordnen (see page 517).

Allgemeine Informationen zu administrativen Aufgaben finden Sie unter Administrative Aufgaben - Zeitlich geplante Aktionen für die IGEL UMS konfigurieren (see page 597).

Weitere Informationen über die Advanced Search in der UMS Web App finden Sie unter Suche nach Geräten in der IGEL UMS Web App (see page 792).

Menüpfad: **UMS Administration > Administrative Aufgaben > Dialog "Eine neue administrative Aufgabe anlegen" > Aktion "Entferne Objektzuordnungen von Geräten von Views / Advanced Searches"**

Allgemein

Name

Name für die Aufgabe.

Aktion:

▶ Wählen Sie **Entferne Objektzuordnungen von Geräten von Views / Advanced Searches**.

Beschreibung
Optionale Beschreibung der Aufgabe.

Sende Ergebnis via Mail

☑ Das Ergebnis der Aufgabe wird per E-Mail an die festgelegten Empfänger gesendet.

Die folgenden zwei Optionen sind aktiv, falls **Sende Ergebnis via Mail** aktiviert ist:

An Hauptempfänger senden (nicht definiert)

☑ Die E-Mail wird an die unter **E-Mail-Einstellungen > E-Mail-Empfänger** definierte E-Mail-Adresse gesendet. Weitere Informationen finden Sie unter E-Mail-Einstellungen (see page 664).

E-Mail-Empfänger
Weitere E-Mail-Adressen, an die die E-Mail gesendet wird. Wenn Sie mehrere Adressen eingeben, müssen Sie diese mit Semikolon ";" voneinander abtrennen.

Aktiv

☑ Die Aufgabe wird zum eingestellten Zeitpunkt ausgeführt. (Standard)

☐ Die Aufgabe wird nicht ausgeführt.

Views / Geräte-Suchen auswählen

▶ Wählen Sie eine View / Geräte-Suche / Advanced Search und klicken Sie auf  um sie zu der Liste hinzuzufügen, von denen ein oder mehrere zugewiesenen Objekte entfernt werden müssen.

Objekte auswählen

▶ Wählen Sie eine Objekte aus und klicken Sie auf  um sie zu der Liste hinzuzufügen, die Sie von den Views oder Geräte-Suchen entfernen wollen.

Objekte können sein:

- Profile
- Firmwareanpassungen
- Dateien
- Firmwareupdates

Serverzuordnung

> ⓘ Die Seite "**Serverzuordnung**" wird nur bei der Verwendung der High-Availability- oder Distributed UMS (see page 246)-Umgebung angezeigt.

Zuordnungstyp

Mögliche Optionen:

- **Ein Server (zufällige Auswahl)**: Der Server für diese Aufgabe wird automatisch aus den unter **Zugeordnete Server** aufgelisteten Servern ausgewählt.
- **Ein Server (direkte Zuordnung)**: Sie können einen bestimmten Server für diese Aufgabe auswählen. Die verfügbaren Server sind unter **Zugeordnete Server** aufgelistet.
- **Alle Server**: Die Aufgabe wird von allen Servern durchgeführt.

Zugeordnete Server

Liste von Servern, die für diese Aufgabe verfügbar sind.

Zeitplan

Start
Zeitpunkt, an dem die Aufgabe ausgeführt wird.

Aufgabe startet alle [Anzahl Zeiteinheiten]

☑ Die Aufgabe wird im eingestellten Zeitintervall wiederholt.

☐ Die Aufgabe wird nicht im eingestellten Zeitintervall wiederholt.

Wochentage
Die Aufgabe wird an den aktivierten Wochentagen zum unter **Start** definierten Zeitpunkt ausgeführt.

Monatlich
Die Aufgabe wird monatlich zum unter **Start** angegebenen Zeitpunkt ausgeführt.

Feiertage ausschließen
Die Aufgabe wird nicht ausgeführt an den Tagen, die in den über ... ausgewählten Feiertagslisten aufgelistet sind. Weitere Informationen zu den Feiertagslisten finden Sie in der Menüleiste unter **Extras > Geplante Aufgaben**, siehe Menüleiste der IGEL UMS Konsole (see page 343).

Ende
Zeitpunkt, ab dem die Aufgabe nicht mehr wiederholt wird.

Verlauf der Assetinformationen löschen

Sie können das Löschen des Verlaufs der Assetinformationen (see page 963) als administrative Aufgabe definieren. Die Löschung hilft bei der Leistungsoptimierung, siehe Leistungsoptimierungen (see page 294).

Menüpfad: **UMS Administration > Administrative Aufgaben >** Dialog **Eine neue administrative Aufgabe anlegen > Aktion "Verlauf der Assetinformationen löschen"**

Allgemein

Name

Name für die Aufgabe.

Aktion

▶ Wählen Sie **Verlauf der Assetinformationen löschen**.

Beschreibung
Optionale Beschreibung der Aufgabe.

Sende Ergebnis via Mail

☑ Das Ergebnis der Aufgabe wird per E-Mail an die festgelegten Empfänger gesendet.

Die folgenden zwei Optionen sind aktiv, falls **Sende Ergebnis via Mail** aktiviert ist:

An Hauptempfänger senden (nicht definiert)

☑ Die E-Mail wird an die unter **E-Mail-Einstellungen > E-Mail-Empfänger** definierte E-Mail-Adresse gesendet. Weitere Informationen finden Sie unter E-Mail-Einstellungen (see page 664).

E-Mail-Empfänger
Weitere E-Mail-Adressen, an die die E-Mail gesendet wird. Wenn Sie mehrere Adressen eingeben, müssen Sie diese mit Semikolon ";" voneinander abtrennen.

Aktiv

☑ Die Aufgabe wird zum eingestellten Zeitpunkt ausgeführt. (Standard)

☐ Die Aufgabe wird nicht ausgeführt.

Konfiguration

Verzeichnis für exportierte Dateien

Verzeichnis auf dem UMS Server, in dem die Assetinformationen gesichert werden sollen. Wenn Sie das Feld leer lassen, wird das Verzeichnis `C:/Program Files/IGEL/RemoteManager/rmguiserver/temp` verwendet.

Löscheinstellungen der Historie

Lösche Asset-Info-Historie älter als

Angabe in Tagen, wie alt die zu löschenden Informationen sein sollen. (Standard: 5)

Lösche nur unbenutzte Assets

☑ Nur unbenutzte Assets werden im angegebenen Zeitraum gelöscht. (Standard)

☐ Alle Assets werden im angegebenen Zeitraum gelöscht.

Zeitplan

Start
Zeitpunkt, an dem die Aufgabe ausgeführt wird.

Aufgabe startet alle [Anzahl Zeiteinheiten]

☑ Die Aufgabe wird im eingestellten Zeitintervall wiederholt.

☐ Die Aufgabe wird nicht im eingestellten Zeitintervall wiederholt.

Wochentage
Die Aufgabe wird an den aktivierten Wochentagen zum unter **Start** definierten Zeitpunkt ausgeführt.

Monatlich
Die Aufgabe wird monatlich zum unter **Start** angegebenen Zeitpunkt ausgeführt.

Feiertage ausschließen
Die Aufgabe wird nicht ausgeführt an den Tagen, die in den über ... ausgewählten Feiertagslisten aufgelistet sind. Weitere Informationen zu den Feiertagslisten finden Sie in der Menüleiste unter **Extras > Geplante Aufgaben**, siehe Menüleiste der IGEL UMS Konsole (see page 343).

Ende
Zeitpunkt, ab dem die Aufgabe nicht mehr wiederholt wird.

Sende Benachrichtigungen via E-Mail

Sie können in der IGEL Universal Management Suite (UMS) eine administrative Aufgabe definieren, durch die Benachrichtigungen per E-Mail versendet werden. Details zu den Benachrichtigungen finden Sie unter Benachrichtigungen in der IGEL UMS konfigurieren (see page 221).

Allgemeine Informationen zu administrativen Aufgaben finden Sie unter Administrative Aufgaben - Zeitlich geplante Aktionen für die IGEL UMS konfigurieren (see page 597).

Menüpfad: **UMS Administration > Globale Konfiguration > Administrative Aufgaben >** Dialog **Eine neue administrative Aufgabe anlegen >** Aktion **"Sende Benachrichtigungen via E-Mail"**

Allgemein

Name

Name für die Aufgabe.

Aktion

▶ Wählen Sie **Sende Benachrichtigungen via E-Mail**.

Beschreibung
Optionale Beschreibung der Aufgabe.

Sende Ergebnis via Mail

☑ Das Ergebnis der Aufgabe wird per E-Mail an die festgelegten Empfänger gesendet.

Die folgenden zwei Optionen sind aktiv, falls **Sende Ergebnis via Mail** aktiviert ist:

An Hauptempfänger senden (nicht definiert)

☑ Die E-Mail wird an die unter **E-Mail-Einstellungen > E-Mail-Empfänger** definierte E-Mail-Adresse gesendet. Weitere Informationen finden Sie unter E-Mail-Einstellungen (see page 664).

E-Mail-Empfänger
Weitere E-Mail-Adressen, an die die E-Mail gesendet wird. Wenn Sie mehrere Adressen eingeben, müssen Sie diese mit Semikolon ";" voneinander abtrennen.

Aktiv

☑ Die Aufgabe wird zum eingestellten Zeitpunkt ausgeführt. (Standard)

☐ Die Aufgabe wird nicht ausgeführt.

Konfiguration

E-Mail-Empfänger

E-Mail-Adresse, zu der die Nachricht versendet werden soll.

Exportformat

Datenformat, in dem die Ergebnisse der Aufgabe als E-Mail-Anhang verschickt werden.
Mögliche Optionen:

- **XML** (Standard)
- **HTML**
- **CSV**

Archiv erstellen

☑ Es wird ein Archiv angelegt.

☐ Es wird kein Archiv angelegt. (Standard)

Exportiere

Legt fest, ob alle oder nur neue Benachrichtigungen exportiert werden sollen.
Mögliche Optionen:

- **Alle Benachrichtigungen** (Standard)
- **Nur Benachrichtigungen, die nach der letzten Ausführung der Admin-Aufgaben generiert wurden**

Exportiere Benachrichtigungen über

Legt fest, welche Benachrichtigungstypen exportiert werden sollen. Mehr über die Benachrichtigungstypen erfahren Sie unter Benachrichtigungen in der IGEL UMS konfigurieren (see page 221).
Mögliche Optionen:

- **Universal Firmware Updates (bis OS 11.07)**
- **Universal Firmware Updates - Stable Releases**
- **Universal Firmware Updates - Rolling Releases**

  ⓘ Bereits existierende administrative Aufgaben mit aktivierten **Universal Firmware Updates** (d.h. die, die vor dem Update auf UMS 12 erstellt wurden) werden automatisch in **Universal Firmware Updates (bis OS 11.07)** und **Universal Firmware Updates - Stable Releases** konvertiert. **Universelle Firmware Updates - Rolling Releases** sind standardmäßig deaktiviert.

- **Universal Management Lizenzen**
- **Gerätelizenzen**

- **Speicherplatzverbrauch**
- **Globale Benachrichtigungen**
- **Admin-Aufgaben**
- **Packs**
- **Zertifikate**

Zeitplan

Start
Zeitpunkt, an dem die Aufgabe ausgeführt wird.

Aufgabe startet alle [Anzahl Zeiteinheiten]

☑ Die Aufgabe wird im eingestellten Zeitintervall wiederholt.

☐ Die Aufgabe wird nicht im eingestellten Zeitintervall wiederholt.

Wochentage
Die Aufgabe wird an den aktivierten Wochentagen zum unter **Start** definierten Zeitpunkt ausgeführt.

Monatlich
Die Aufgabe wird monatlich zum unter **Start** angegebenen Zeitpunkt ausgeführt.

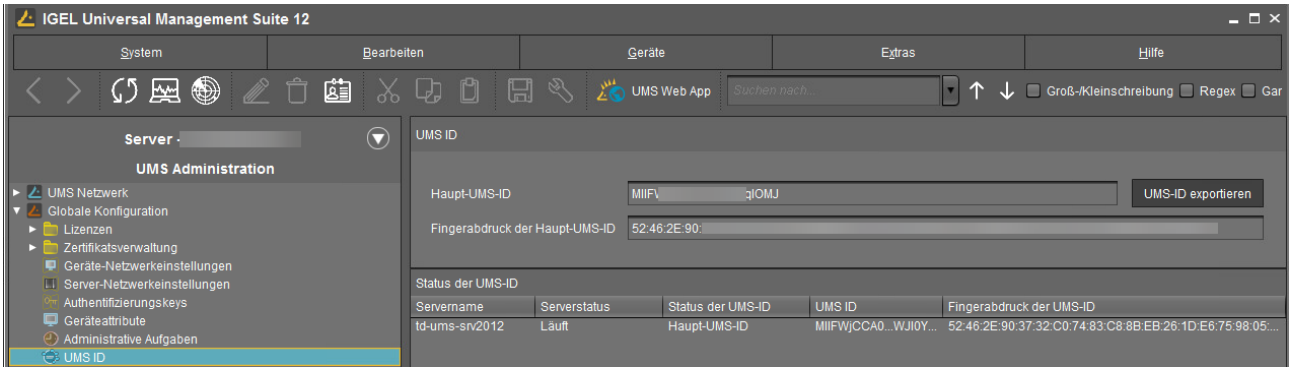
Feiertage ausschließen
Die Aufgabe wird nicht ausgeführt an den Tagen, die in den über ... ausgewählten Feiertagslisten aufgelistet sind. Weitere Informationen zu den Feiertagslisten finden Sie in der Menüleiste unter **Extras > Geplante Aufgaben**, siehe Menüleiste der IGEL UMS Konsole (see page 343).

Ende
Zeitpunkt, ab dem die Aufgabe nicht mehr wiederholt wird.

UMS ID

Im folgenden Artikel finden Sie Informationen über die UMS-ID (vor UMS 12 als "UMS-Lizenz-ID" bezeichnet), die Sie in Ihrer IGEL Universal Management Suite (UMS) Installation finden können.

Menüpfad: **UMS Adminisration > Globale Konfiguration > UMS ID**



Die UMS-ID wird z. B. für die Kommunikation Ihrer UMS mit den IGEL Cloud Services benötigt.

Die UMS-ID ermöglicht auch die Kommunikation zwischen der UMS und dem IGEL Lizenz-Portal (ILP).

Die UMS-ID erlaubt vollständiges Automatic License Deployment (ALD), d.h. eine automatische Bereitstellung von Lizenzen, ohne dass bei jedem Kauf von Lizenzen ein ALD Token verarbeitet werden muss. Hierzu muss die UMS-ID beim IGEL Lizenz-Portal registriert werden. Weitere Informationen finden Sie unter Automatic License Deployment (ALD) einrichten.

Die UMS-ID besteht aus einem öffentlich/privaten Schlüsselpaar. Der öffentliche Schlüssel ist ein Zertifikat und kann als `.crt`-Datei exportiert werden. Die Registrierung der UMS-ID geschieht durch das Hochladen der Zertifikatsdatei in das IGEL Lizenz-Portal.

Eine UMS-ID wird nicht beeinflusst oder geändert, wenn die UMS-Datenbank von einem Backup wiederhergestellt wird. Die UMS-ID ändert sich nicht, wenn Parameter der UMS-Installation geändert werden, beispielsweise Hostname/IP-Adresse. Somit ist sie auf einen beliebigen anderen Server übertragbar.

Sicherungsmöglichkeiten der UMS-ID finden Sie unter UMS-ID-Sicherung im IGEL Administrator (see page 713) oder IGEL UMS Administrator Kommandozeilenschnittstelle (see page 740).

UMS-ID

> Die UMS-ID wird bei jeder Installation eines UMS Servers erzeugt. Wenn Sie also eine High-Availability- oder Distributed UMS-Umgebung (siehe IGEL UMS Installation (see page 246)) haben, hat jeder Server eine eigene UMS-ID, d. h. eine **lokale UMS-ID**. Für die Kommunikation aller UMS Server mit dem ILP und den IGEL Cloud Services wird eine **Haupt-UMS-ID** verwendet. Daher muss die **Haupt-UMS-ID** zwischen allen Servern synchronisiert werden, siehe Status der UMS-ID (see page 640) unten.

Haupt-UMS-ID: Die UMS-ID, die für die Kommunikation mit dem ILP und den IGEL Cloud Services verwendet wird. Die ersten und letzten 10 Zeichen werden angezeigt.

UMS-ID exportieren: UMS-ID als `.crt` -Datei exportieren.

Fingerabdruck der Haupt-UMS-ID: Der SHA-256-Fingerabdruck der UMS-ID.

Status der UMS-ID

Wenn Sie einen einzelnen Server betreiben, wird in diesem Bereich der Status der UMS-ID für diesen Server angezeigt.

Wenn Sie eine UMS High Availability- oder Distributed UMS-Umgebung betreiben, werden in diesem Bereich die Status der UMS-ID für jeden Server der UMS-Installation aufgelistet. Jeder Server erhält die UMS-ID beim Start oder Neustart.

Servername: Name des Hostservers, wie unter **UMS Administration > UMS Netzwerk > Server** angezeigt.

Serverstatus: Status des Servers, z. B. "Läuft".
Mögliche Werte:

- 'Läuft'
- 'Ist aus'

Status der UMS-ID: Zeigt an, ob der Server die aktuelle Haupt-UMS-ID hat oder nicht. Wenn er die Haupt-UMS-ID hat, zeigt das Feld "Haupt-UMS-ID" oder "Synchron". Wenn nicht, muss der Server neu gestartet werden, um sich zu synchronisieren.
Mögliche Werte:

- 'Haupt-UMS-ID'
- 'Synchron'
- 'Nicht synchron, bitte Server neustarten'

> Wenn der Neustart nicht hilfreich war, muss die UMS-ID manuell synchronisiert werden, siehe Manuelle Synchronisierung der UMS-ID (see page 157).

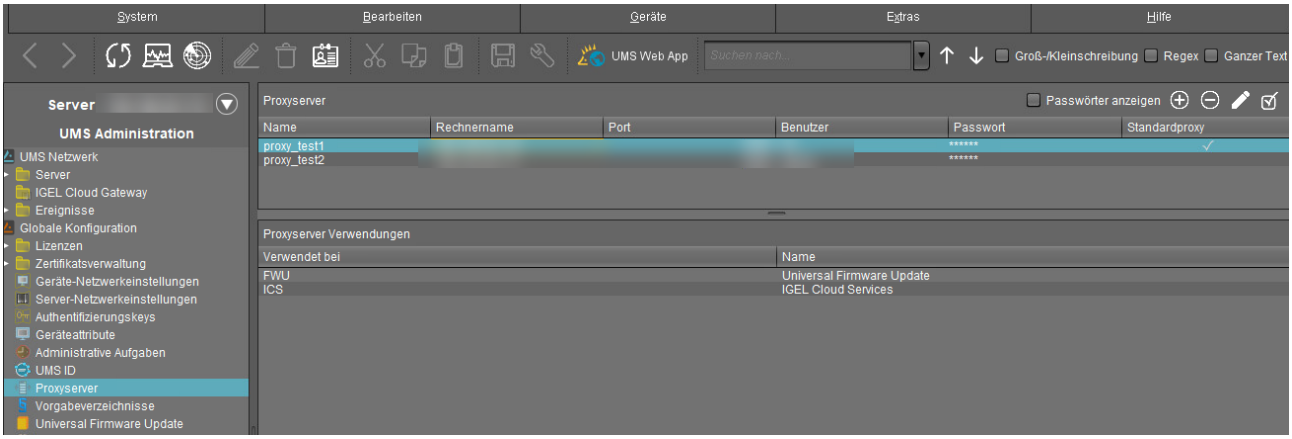
UMS-ID: Die aktuell auf dem Server verwendete UMS-ID. Die ersten und letzten 10 Zeichen werden angezeigt.

Fingerabdruck der UMS-ID: Der SHA-256-Fingerabdruck der UMS-ID.

Proxyserver

In der IGEL Universal Management Suite (UMS) können Sie Proxyserver konfigurieren.

Menüpfad: **UMS Konsole > UMS Administration > Globale Konfiguration > Proxyserver**



In diesem Bereich können Sie Proxyserver hinzufügen und konfigurieren, um sie bei folgenden Anwendungsfällen einzusetzen:

- IGEL Cloud Gateway (see page 556)
- IGEL Cloud Services (Beachten Sie, dass ein unter **UMS Administration > Globale Konfiguration > Lizenzen > Verteilung > Proxykonfiguration bearbeiten** definierter Proxy nicht nur für die automatische Lizenzverteilung (see page 565), d.h. nicht nur für die Kommunikation mit dem IGEL Lizenzportal, sondern für alle IGEL Cloud Services, einschließlich IGEL Onboarding Service, IGEL Insight Service, IGEL App Portal sowie für UMS as an Update Proxy (see page 889) verwendet wird)
- Universal Firmware Update (1) (see page 641) (falls konfiguriert, wird dieser Proxy auch für die UMS Update Überprüfung (see page 352) verwendet)

> ⓘ Die Anwendungsfälle IGEL Cloud Services und Universal Firmware Update werden automatisch mit dem Standardproxyserver verbunden.
> Die Einstellungen des IGEL Cloud Gateway werden nicht verändert; der Proxyserver muss manuell hinzugefügt werden.

Proxyserver

In dieser Liste werden alle konfigurierten Proxyserver angezeigt.

Passwörter anzeigen

☑ Passwörter werden in der Liste sichtbar gemacht.

☐ Passwörter werden nicht angezeigt. (Standard)

	Proxyserver hinzuzufügen
	Proxyserver zu löschen
	Proxyserver bearbeiten
	ausgewählten Proxyserver als Standardserver definieren

Es können nur Proxyserver gelöscht werden, die nicht verwendet werden. Der als erstes hinzugefügte Proxyserver wird automatisch als Standardproxyserver geführt.

Proxyserver Verwendungen

In dieser Liste werden alle Verwendungen für den ausgewählten Proxyserver angezeigt.

Die Einträge in dieser Liste erscheinen automatisch, sobald eine Anwendung mit einem ausgewählten Proxyserver verbunden wurde.

Vorgabeverzeichnisse

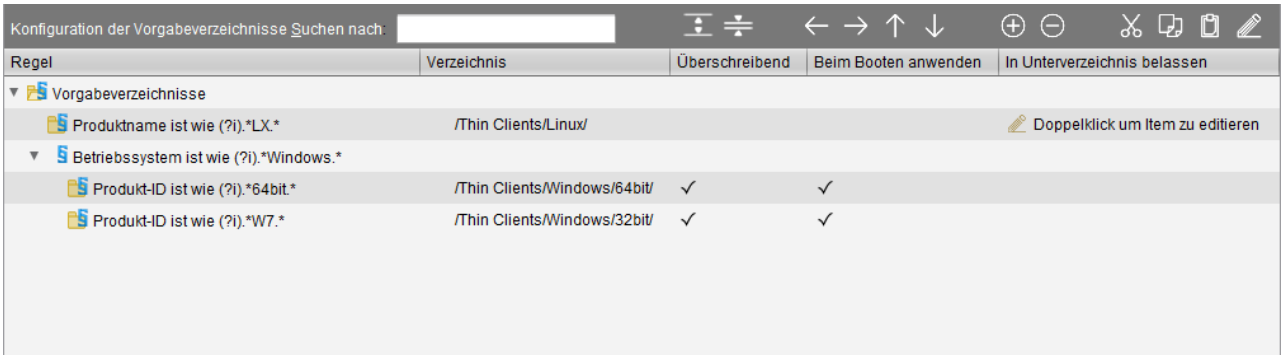
Menüpfad: **UMS Administration > Globale Konfiguration** > **Vorgabeverzeichnisse**

Regeln für Vorgabeverzeichnisse dienen dazu, Geräte bei der Registrierung automatisch in bestimmte Verzeichnisse einzuordnen. Diese Verzeichnisse lassen sich mit Profilen verknüpfen, die dann den enthaltenen Geräten zugewiesen werden. So können Sie die Geräte also automatisch bei der Registrierung konfigurieren (Zero-Touch Deployment).

Siehe auch folgende weiterführende How-Tos:

- Vorgabeverzeichnisregel erstellen (see page 645)
- Verwendung von Struktur-Tags mit IGEL OS 11 Geräten (see page 86)

▶ Gehen Sie zu **UMS Administration > Globale Konfiguration > Vorgabeverzeichnisse**.
Die Benutzeroberfläche sieht so aus:



Wenn Sie mit UMS *Version 5.03.100* oder neuer erstmals eine UMS Datenbank einer älteren Version öffnen, werden die Vorgabeverzeichnisregeln automatisch in die neue Struktur konvertiert. Dabei werden Regeln zum IP-Bereich in zwei Regeln (IP-Bereich von und IP-Bereich bis) aufgetrennt.

- Symbolleiste (see page 644)
- Vorgabeverzeichnisregel erstellen (see page 645)
- Verzeichnisregeln finden (see page 648)
- Verzeichnisregeln anwenden (see page 649)
- Verzeichnisregel bearbeiten (see page 650)
- Bedingungen kombinieren (see page 651)
- Mit Netzmaske arbeiten (see page 653)

Symbolleiste

Menüpfad: **UMS Administration > Globale Konfiguration > Vorgabeverzeichnisse**

In der Symbolleiste für Vorgabeverzeichnisregeln finden Sie Schaltflächen für häufig verwendete Befehle:

In der Reihenfolge der Symbole sind dies:

	Suchen (in allen Spalten)
	Alle Regeln ausklappen
	Alle Regeln einklappen
	Regel eine Ebene höher schieben
	Regel eine Ebene tiefer schieben
	Regel in der Reihenfolge nach oben schieben
	Regel in der Reihenfolge nach unten schieben
	Regel hinzufügen (als letztes Kind der derzeit ausgewählten Regel)
	Regel löschen (inklusive untergeordneter Regeln)
	Objekte ausschneiden
	Objekte kopieren
	Objekte einfügen
	Bearbeiten

Vorgabeverzeichnisregel erstellen

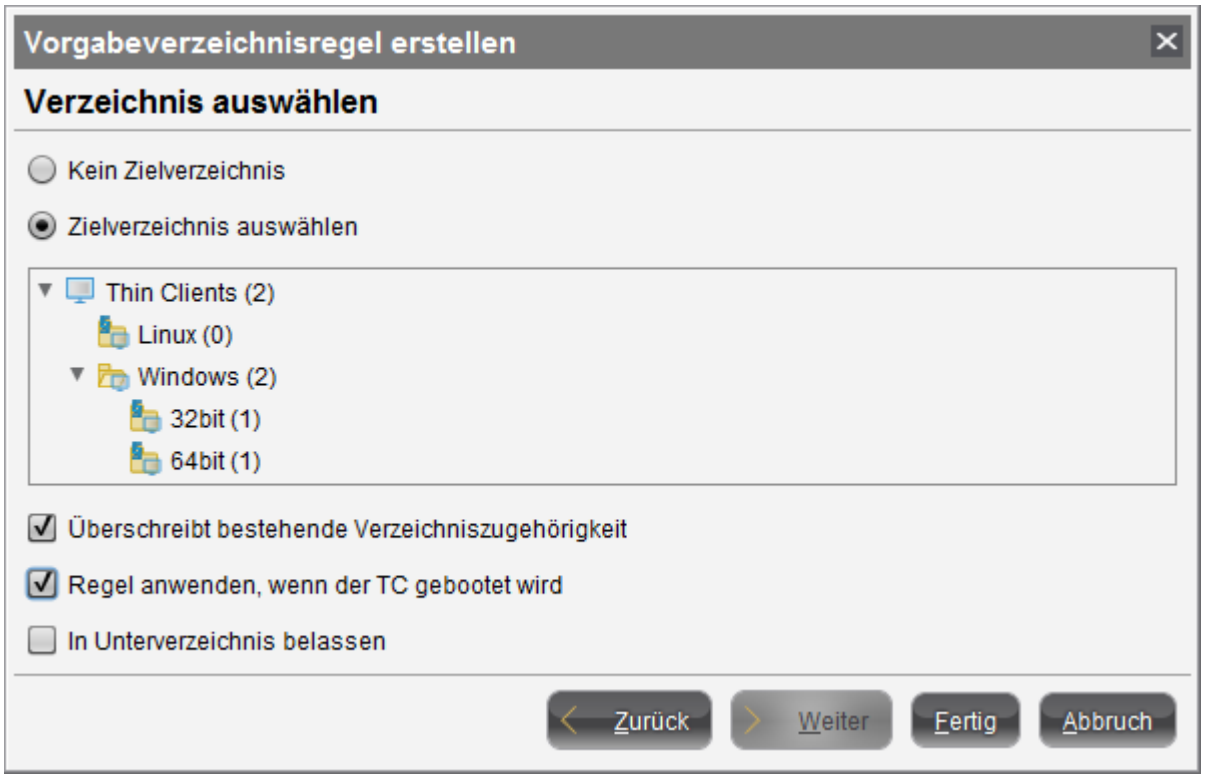
Menüpfad: **UMS Administration > Globale Konfiguration > Vorgabeverzeichnisse**

1. Klicken Sie das Symbol .
2. Der Dialog **Vorgabeverzeichnisregel erstellen** öffnet sich.
3. Wählen Sie einen **Suchparameter** aus. Dabei hilft Ihnen ein Suchfeld, das die Auswahl beim Eintippen auf passende Parameternamen einschränkt.

4. Legen Sie Vergleichswert und Vergleichsoperator für das Kriterium fest.

> ⓘ Wenn Sie eine Regel anlegen, die einen Bereich (von - bis) enthält, wird diese automatisch in ein Paar mit UND verknüpfter Regeln (von UND bis) umgewandelt. Das trifft beispielsweise auf Datums- oder IP-Bereiche zu.

5. Wählen Sie ein Zielverzeichnis aus (muss bereits angelegt sein) oder wählen Sie die Option **Kein Zielverzeichnis**.
   Bei der Option **Zielverzeichnis auswählen** haben Sie folgende weitere Optionen:
   - **Überschreibt bestehende Verzeichniszugehörigkeit**
     ☑ Ein bereits registriertes Gerät wird neu im Zielverzeichnis registriert.
   - **Regel anwenden, wenn der TC gebootet wird**
     ☑ Die Regel wird nicht nur beim Registrieren, sondern auch bei jedem Booten der Geräte angewendet.
   - **In Unterverzeichnis belassen**
     ☑ Ein Gerät wird nicht verschoben, wenn er sich bereits in einem Unterverzeichnis des Zielverzeichnisses befindet.



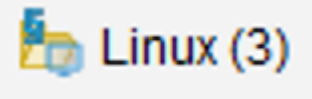
6. Schließen Sie das Erstellen mit einem Klick auf **Fertig** ab.

> Die Reihenfolge der Regeln ist wichtig: Generell wird für jedes Gerät der Vorgabeverzeichnisbaum von oben nach unten durchgegangen. Trifft das Kriterium einer Regel zu und besitzt diese ein Zielverzeichnis, werden deren Kindregeln untersucht. Trifft keine der Kindregeln zu, wird das Gerät in das Zielverzeichnis der obigen Regel verschoben. Trifft jedoch eine der Kindregeln zu und besitzt sie ein Zielverzeichnis, wird diese Kindregel als neue Ausgangsregel hergenommen und die Suche beginnt von Neuem. Besitzt eine zutreffende Regel kein Zielverzeichnis, werden deren Kindregeln untersucht.

Verzeichnisregeln finden

Nur ab UMS Version 5.03.100:

Sie können im Strukturbaum sehen, welche Verzeichnisse Ziel einer Vorgabeverzeichnisregel sind. Das Ordnersymbol trägt dann ein kleines §-Zeichen:



> Ein Verzeichnis, das Ziel einer Vorgabeverzeichnisregel ist, lässt sich nicht löschen. Um es zu löschen, müssen Sie erst die Verzeichnisregel ändern oder löschen.

So springen Sie vom Verzeichnis direkt zu verknüpften Regeln:

1. Führen Sie einen Rechtsklick auf das Ordnersymbol aus.
2. Wählen Sie im Kontextmenü **Suche Vorgabeverzeichnisregeln.**
   Die Ansicht wechselt zur Übersicht der Vorgabeverzeichnisregeln, die erste verknüpfte Regel ist markiert.
3. Drücken Sie die Eingabetaste, um zu weiteren gefundenen Regeln zu springen.

Verzeichnisregeln anwenden

Die Regeln können unabhängig vom Import neuer Clients oder vom Booten bestehender Clients angewendet werden:

Ab UMS Version 5.03.100:

1. Rechtsklicken Sie auf **Vorgabeverzeichnisse** unter **UMS Administration > Globale Konfiguration**.
2. Wählen Sie **Regeln jetzt anwenden ...**
   Ein Dialog mit weiteren Optionen öffnet sich.
3. Wählen Sie aus den Optionen:
   - **Alle bestehenden Verzeichniszugehörigkeiten überschreiben**
     ☑ Ein bereits registriertes Gerät wird neu im Zielverzeichnis registriert.
   - **Ablageort für Geräte ohne gültige Regel:**
     - Im aktuellen Verzeichnis belassen
     - Basisverzeichnis für Geräte
     - Anderes Verzeichnis (auswählen)
4. Klicken Sie **Anwenden**, um die Regeln anzuwenden.

Vor UMS Version 5.03.100:

1. Klicken Sie die Schaltfläche **Regeln jetzt anwenden ...** in der Übersicht der Verzeichnisregeln.
   Ein Dialog mit weiteren Optionen öffnet sich.
2. Wählen Sie aus den Optionen:
   - **Alle bestehenden Verzeichniszugehörigkeiten überschreiben**
     ☑ Ein bereits registriertes Gerät wird neu im Zielverzeichnis registriert.
   - **Ablageort für Geräte ohne gültige Regel:**
     - Im aktuellen Verzeichnis belassen
     - Basisverzeichnis für Geräte
     - Anderes Verzeichnis (auswählen)
3. Klicken Sie **Anwenden**, um die Regeln anzuwenden.

Verzeichnisregel bearbeiten

Ab UMS Version 5.03.100:

▶ Doppelklicken Sie in der Regelübersicht auf eine Zeile ...

- in der Spalte **Regel**, um **Kriterium**, **Operator** und **Wert** zu bearbeiten.
- in der Spalte **Verzeichnis**, um das Zielverzeichnis zu ändern oder zu entfernen.
- in den Spalten **Überschreibend**, **Beim Booten anwenden** oder **In Unterverzeichnis belassen**, um diese Option (see page 645) zu ändern.

Vor UMS Version 5.03.100:

1. Markieren Sie die gewünschte Regel in der Übersicht durch einen einfachen Klick.
2. Klicken Sie das Symbol 
   Das Fenster **Vorgabeverzeichnisregel ändern** öffnet sich.
3. Ändern Sie gemäß Ihren Wünschen **Verzeichnis**, **Kriterium**, **Operator**, **Wert** und Optionen.
   Weitere Bedingungen mit UND- oder ODER-Verknüpfung können Sie hier ebenfalls hinzufügen, siehe Bedingungen kombinieren (see page 651).

Bedingungen kombinieren

In der *UMS* können Sie die Bedingungen von Verzeichnisregeln mittels UND- und ODER-Verknüpfungen kombinieren.

Ab UMS Version 5.03.100:

▶ Rücken Sie eine Regel mittels  ein, um eine UND-Verknüpfung mit der Bedingung der übergeordneten Regel zu erreichen:

Beispiel: In der Abbildung werden Geräte in das Verzeichnis `/Geräte/Windows/64bit/` verschoben, deren **Produkt-ID** `Windows` UND `64bit` enthält.

> ⓘ Sie können Regeln, die kein Zielverzeichnis besitzen (Linking Rules), verwenden, um Bedingungen miteinander zu kombinieren.

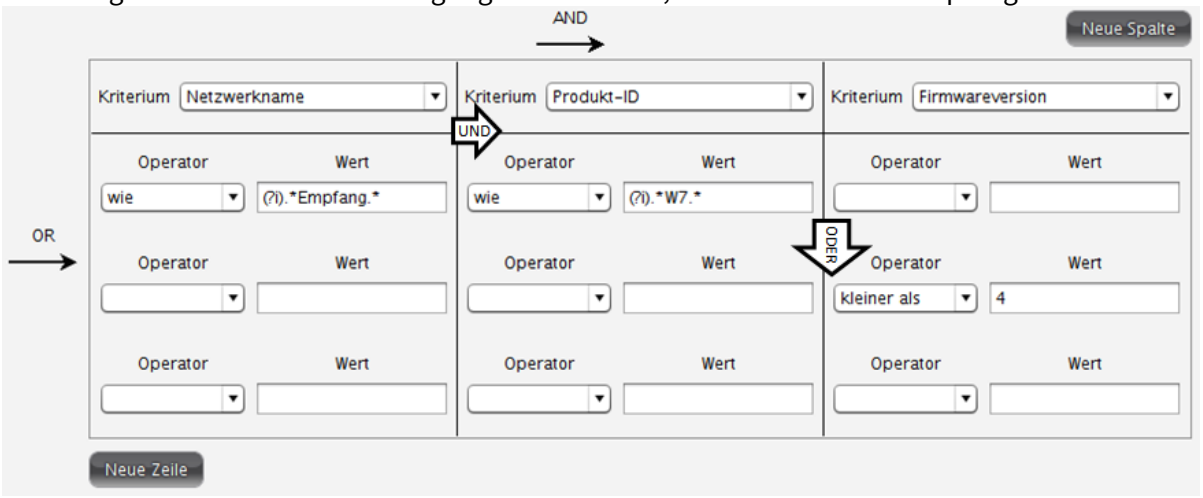
▶ Lassen Sie Regeln gleich weit eingerückt und weisen Sie ihnen dasselbe Zielverzeichnis zu, um eine ODER-Verknüpfung der Bedingungen zu erreichen:

Beispiel: In der Abbildung werden Geräte in das Verzeichnis `/Geräte/Windows/64bit/` verschoben, deren **Produkt-ID** `64bit` ODER `W10` enthält.

> Sie können Regeln sowie Gruppen von Regeln per Drag-and-Drop verschieben sowie mittels der Symbolleiste kopieren und einfügen.

Vor UMS Version 5.03.100:

- Beim Hinzufügen einer neuen Regel:
  - Wählen Sie **Suche weiter einschränken** im Assistenten, um eine UND-verknüpfte Bedingung hinzuzufügen.
  - Wählen Sie **Weiteres Auswahlkriterium festlegen** um eine ODER-verknüpfte Bedingung hinzuzufügen.
- Beim Bearbeiten einer bestehenden Regel:
  - Fügen Sie eine weitere Bedingung auf der rechten Seite ein, um eine UND -Verknüpfung zu erreichen.
  - Fügen Sie eine weitere Bedingung unterhalb ein, um eine ODER-Verknüpfung zu erreichen.



Mit Netzmaske arbeiten

Wählen Sie beim Erstellen einer Verzeichnisregel das Kriterium **Netzmaske**, so werden die Thin Clients nach IP-Adressbereichen in automatisch angelegte Verzeichnisse einsortiert. Der Name des Ordners wird durch diese bitweise Operation ermittelt:

```
Ordner = IP-Adresse des Thin Clients AND Netzmaske
```

Beispiele:

IP-Adresse	Netzmaske	Resultierendes Verzeichnis
`130.094.122.195`	`255.255.255.224`	`130.094.122.192`
`172.16.232.15`	`255.255.0.0`	`172.16.0.0`
`192.168.1.1`	`255.255.255.0`	`192.168.1.0`

Als **Zielverzeichnis** wählen Sie das Geräteverzeichnis, unter dem die Unterordner für die IP-Adressbereiche angelegt werden sollen.

Da diese Regel immer zutrifft, ist es nicht sinnvoll, eine weitere Regel zu definieren. Wenn die Netzmaskenregel alle Geräte in Verzeichnisse sortiert, ist keine weitere Regel aktiv.

Wake-on-LAN

Geräte lassen sich mittels Magic Packets über das Netzwerk aufwecken. Ein Magic Packet beinhaltet die MAC-Adressen der Geräte, die aufzuwecken sind. Voraussetzung für das Aufwecken eines Geräts ist, dass dieser sich in einem der Zustände S3 (Suspend-to-RAM – STR), S4 (Suspend-to-Disk – STD) oder S5 (Soft-Off) befindet. In der UMS Administration können Sie festlegen, an welche Netzwerkadressen die Magic Packets verschickt werden.

Für Szenarien, in denen sich die UMS außerhalb des Netzwerks der Geräte befindet und Broadcast-Pakete aus dem WAN nicht zugelassen sind, können Sie einen oder mehrere Linux Geräte als Wake-on-LAN-Proxy definieren.

> ⓘ Die Funktionalität Wake-on-LAN-Proxy wird von Linux Geräten ab Version 5.09.100 unterstützt.

Menüpfad: **UMS Administration > Globale Konfiguration > Wake-on-LAN**

Broadcast-Adresse

☑ Das Magic Packet wird an die Broadcast-Adresse des Netzwerks gesendet.

Letzte bekannte IP-Adresse des Geräts

☑ Das Magic Packet wird an die letzte bekannte IP-Adresse des Geräts gesendet.

Automatische Wake-on-LAN-Proxy-Erkennung

☐ Falls im Subnetz ein anderes Gerät verfügbar ist, dann wird dieser als Wake-on-LAN-Proxy verwendet.

Alle bekannten Subnetze

☑ Das Magic Packet wird an die Netzwerkadressen aller Subnetze gesendet, die der UMS bekannt sind.

☐ Das Magic Packet wird nicht an die Netzwerkadressen aller Subnetze gesendet, die der UMS bekannt sind. (Standard)

So fügen Sie ein Subnetz hinzu:

1. Aktivieren Sie **Alle bekannten Subnetze**.
2. Klicken Sie im Bereich unterhalb von **Alle bekannten Subnetze** auf ⊕.
   Der Dialog **Subnetze definieren** öffnet sich.
3. Geben Sie im Feld **Subnetz** die Netzwerkadresse des Subnetzes ein.
4. Wählen Sie unter **CIDR** (Classless Inter-Domain Routing) das passende Suffix für die Netzwerkmaske aus.

> Sinnvoll sind Werte zwischen 8 und 28. Beispiel 1: Die Netzwerkadresse `10.43.8.0` mit dem Suffix 24 entspricht der CIDR-Notation `10.43.8.0/24` mit der Netzmaske `255.255.255.0`. Dieses Netzwerk entspricht einem Klasse-C-Netzwerk. Die für Hosts nutzbaren Adressen liegen zwischen `10.43.8.1` und `10.43.8.254`. Beispiel 2: Die Netzwerkadresse `10.43.8.64` mit dem Suffix 28 entspricht der CIDR-Notation `10.43.8.64/28` mit der Netzmaske `255.255.255.240`. Die für Hosts nutzbaren Adressen liegen zwischen `10.43.8.65` und `10.43.8.78`.

5. Fügen Sie gegebenenfalls einen **Kommentar** hinzu.
6. Klicken Sie **Ok**.

Netzwerkadresse der letzten bekannten IP

☑ Das Magic Packet wird an die Netzwerkadresse des Netzwerks gesendet, in dem sich die letzte bekannte IP-Adresse des Geräts befindet. Damit diese Netzwerkadresse ermittelt werden kann, müssen Sie für die in Frage kommenden Netzwerke jeweils eine Netzwerkmaske angeben.

So fügen Sie eine Netzwerkmaske hinzu:

1. Klicken Sie im Bereich unterhalb von **Netzwerkadresse der letzten bekannten IP** auf ⊕.
   Der Dialog **Netzwerkmaske definieren** öffnet sich.
2. Geben Sie die **Netzwerkmaske** ein.
3. Fügen Sie gegebenenfalls einen **Kommentar** hinzu.
4. Klicken Sie **Ok**.

Wake-on-LAN-Proxies

☑ Das Magic Packet wird an die als Wake-on-LAN-Proxy definierten Geräte gesendet. Jeder Wake-on-LAN-Proxy versendet die Magic Packets als Broadcast in dem Netzwerk, in dem er sich befindet.

> Die Einstellungen **Broadcast-Adresse**, **Letzte bekannte IP-Adresse des Geräts**, **Alle bekannten Subnetze** und **Netzwerkadresse der letzten bekannten IP** haben auf den Wake-on-LAN-Proxy keine Auswirkung.

☐ Das Magic Packet wird nicht an die als Wake-on-LAN-Proxy definierten Geräte gesendet.

> Geräte, die als Wake-on-LAN-Proxy konfiguriert sind, behalten ihre Rolle bei, auch wenn **Wake-on-LAN-Proxies** deaktiviert ist.

So definieren Sie einen oder mehrere Geräte als Wake-on-LAN-Proxy:

1. Klicken Sie im Bereich unterhalb von **Wake-on-LAN-Proxies** auf  .
   Der Dialog **Wake-on-LAN-Proxies bearbeiten** öffnet sich.
2. Markieren Sie in der linken Spalte das gewünschte Gerät.
3. Klicken Sie  , um das Gerät zu selektieren.
4. Klicken Sie **Ok**.
   Das Gerät fungiert als Wake-on-LAN-Proxy.

> Ein Gerät, das als Wake-on-LAN-Proxy konfiguriert ist, kann nicht mehr auf Standby gesetzt oder heruntergefahren werden. Diese Sperre tritt in Kraft, sobald das Gerät die Einstellungen von der UMS erhalten hat.

So machen Sie die Konfiguration als Wake-on-LAN-Proxy rückgängig:

1. Klicken Sie im Bereich unterhalb von **Wake-on-LAN-Proxies** auf  .
   Der Dialog **Wake-on-LAN-Proxies bearbeiten** öffnet sich.
2. Markieren Sie in der rechten Spalte das gewünschte Gerät.
3. Klicken Sie  , um das Gerät zu deselektieren.
4. Klicken Sie **Ok**.
   Das Gerät ist nicht mehr als Wake-on-LAN-Proxy konfiguriert, sobald die Einstellung an das Gerät gesendet worden ist.

Active Directory / LDAP

Menüpfad: **UMS Administration > Globale Konfiguration > Active Directory / LDAP**

Die Anbindung des UMS Servers an ein bestehendes Active Directory kann aus zwei Gründen sinnvoll sein:

- Sie möchten Benutzer aus dem AD als UMS Administratorkonten importieren.
- Sie möchten Benutzerprofile über IGEL Shared Workplace einsetzen.

Für beide Einsatzzwecke müssen Sie die jeweiligen Active Directories zuvor im Bereich **UMS Administration** unter **Globale Konfiguration > Active Directory / LDAP** einbinden. Siehe auch das How-To Das Konfigurieren einer AD-Verbindung (see page 184).

1. Wenn Sie Benutzer- und Gruppenabhängigkeiten zwischen verschiedenen konfigurierten Domänen/Subdomänen haben, möchten Sie vielleicht **Alle konfigurierten AD Domains für Suche und Import von AD Usern / Gruppen berücksichtigen** aktivieren. Mit dieser Option wird die Gruppensuche für einen Benutzer innerhalb aller konfigurierten Domänen aktiviert. Bei der Aktivierung wird ein Bestätigungsdialog angezeigt.

   > Wenn diese Option aktiviert ist, kann ein Benutzer zusätzliche Berechtigungen erhalten. Dies ist dann der Fall, wenn
   > - der Benutzer in einer Gruppe ist, die aufgrund dieser Option gefunden wurde,
   > - diese Gruppe unter **System > Administratorkonten** importiert wurde,
   > - und dieser Gruppe Berechtigungen zugewiesen wurden, d. h. Berechtigungen, die der Benutzer sonst nicht haben würde.
   >
   > Bitte beachten Sie, dass diese Option aufgrund der zusätzlichen Suchvorgänge Auswirkungen auf die Performance in den folgenden Bereichen haben kann:
   > - UMS-Anmeldung
   > - Berechtigungsdialoge
   > - Shared Workplace (SWP)

2. Fügen Sie über **Hinzufügen (+)** einen neuen Eintrag zur Liste der angebundenen Active Directories hinzu.
3. Geben Sie den **Domänenname**n an.
4. Geben Sie den/die **Domänencontroller** an.

   > Falls die Option **LDAPS Verbindung** (siehe unten) aktiviert ist, muss ein vollständiger Name des Domänencontrollers (FQDN) eingegeben werden: z. B. `dc01.your.domain`.

   > Um mehrere Domänencontroller voneinander zu trennen, verwenden Sie ein Semikolon.

5. Geben Sie die **Seitengröße** an.
   Die Seitengröße ist eine serverseitige Begrenzung der Treffermenge von Objekten im Active Directory. Der Standardwert ist "1000". Ändern Sie diesen Wert entsprechend Ihrer Serverkonfiguration.
6. Aktivieren Sie **LDAPS Verbindung**, um die Verbindung mit dem angegebenen Zertifikat zu sichern. Der **Port** ändert sich automatisch auf den Standardwert "636".

7. Klicken Sie auf **SSL-Zertifikat importieren**, um das Zertifikat zu konfigurieren und den **Zertifikat-DN** zu verifizieren.

   > Der Name des **Domänencontroller**s und das Zertifikat müssen übereinstimmen, andernfalls schlägt die Verbindung zum LDAP-Server fehl. Siehe Probleme bei der Konfiguration von Active Directory mit LDAPS (see page 196).

   > Falls mehr als ein Domänencontroller verwendet wird, muss ein Stammzertifikat der Domäne konfiguriert werden.

   > Die unterstützten Zertifikatsformate sind `.cer`, `.pem` und `.der`

8. Geben Sie gültige Benutzerdaten unter **Benutzername** und **Passwort** ein.

   > Für den Benutzer reicht eine Leseberechtigung, da keine Änderungen an den AD-Daten vorgenommen werden.

9. Geben Sie Aliase unter **UPN-Suffix** an, falls sie konfiguriert wurden. Beispiel: `domain.local;test.local`
10. Klicken Sie auf **Verbindung testen**, um die Anbindung zu prüfen.

    > Es lassen sich mehrere Active Directories anbinden. Achten Sie daher beim Einloggen, z. B. an der UMS Konsole, auf die Angabe der korrekten Domäne.

    > In diesem Dokument werden die Begriffe "Active Directory" und "LDAP" z.T. synonym verwendet:
    > - Administrative Benutzer / UMS Administratoren lassen sich sowohl aus einem AD wie auch aus einem LDAP heraus importieren.
    > - Shared Workplace-Benutzer können sich lediglich bei einem Active Directory authentifizieren, ein LDAP-Dienst kann hierfür nicht verwendet werden.

11. Klicken Sie auf **Ok**, um die Änderungen zu speichern.

Fernzugriff

In der IGEL Universal Management Suite (UMS) können Sie eine sichere Terminalsitzung und eine sichere VNC-Verbindung global aktivieren.

Menüpfad: **UMS Konsole > UMS Administration > Globale Konfiguration > Fernzugriff**

Sicheres Terminal

Sicheres Terminal global aktivieren

☑ Der Zugriff über das sichere Terminal ist für alle registrierten Geräte aktiviert.

☐ Der Zugriff über das sichere Terminal ist nicht für alle registrierten Geräte aktiviert, kann aber für einzelne Geräte aktiviert werden. (Standard)

Benutzername für sicheres Terminal loggen: Legt fest, ob der Benutzername des UMS Benutzers protokolliert wird, der die Verbindung zum Gerät hergestellt hat. Das Protokoll wird unter **System > Logging > Log sicherer Zugriffe** angezeigt.

☑ Der Benutzername ist im Protokoll enthalten.

☐ Der Benutzername ist nicht im Protokoll enthalten. (Standard)

Sicheres VNC

Sicheres VNC global aktivieren

☑ Der Zugriff über sicheres VNC ist für alle registrierten Geräte aktiviert.

☐ Der Zugriff über sicheres VNC ist nicht für alle registrierten Geräte aktiviert, kann aber für einzelne Geräte aktiviert werden. (Standard)

> **Sicheres Spiegeln und IGEL OS 12**
> Das Shadowing von IGEL OS 12-Geräten über die UMS erfolgt immer über das Unified Protocol und ist daher sicher, d. h. die Kommunikation ist immer verschlüsselt. Standardmäßig wird das Shadowing über das einfache VNC-Protokoll verweigert. Sie können jedoch die Option **Spiegeln mittels externen VNC-Tool verbieten** deaktivieren, wenn Sie möchten, dass die Geräte von einem externer VNC Viewer (see page 485) über das einfache VNC-Protokoll beschattet werden können.

Benutzername für sicheres VNC loggen: Legt fest, ob der Benutzername des UMS Benutzers protokolliert wird, der die Verbindung zum Gerät hergestellt hat. Das Protokoll wird unter **System > Logging > Fernzugriff** angezeigt.

☑ Der Benutzername ist im Protokoll enthalten.

☐ Der Benutzername ist nicht im Protokoll enthalten. (Standard)

Bevorzugte Kodierung
Mögliche Optionen:

- **Tight**
- **Raw**
- **RRE**
- **Hextile**
- **Zlib**

Farbtiefe
Mögliche Werte:

- **24 Bit**
- **8 Bit**

Aktualisierungsperiode: Zeitdauer in Millisekunden, innerhalb derer die Anzeige im VNC-Viewer aktualisiert wird.

Kompressionsstufe: Legt fest, wie stark die übertragenen Daten komprimiert werden.

JPEG-Qualität: Legt die Bildqualität fest.

'Zeichne Rechteck'-Methode verwenden

☑ Die 'Zeichne Rechteck'-Methode wird verwendet. (Standard)

VNC Viewer Einstellungen übersteuern

☑ Die Einstellungen des VNC Viewers werden durch die hier gemachten Einstellungen überschrieben.

☐ Der VNC Viewer kann die hier gemachten Einstellungen überschreiben. (Standard)

Logging

In diesem Bereich können Sie das Protokollierungsverhalten der UMS für Nachrichten und für Ereignisse festlegen sowie Leistungsaufzeichnung aktivieren.

> **UMS Web App**
>
> Protokolle für die in der UMS Web App durchgeführten Aktionen werden nur in der UMS Web App angezeigt. Mehr Informationen zur Protokollierung in der UMS Web App finden Sie unter Logging in der IGEL UMS Web App (see page 903).

Menüpfad: **UMS Administration > Globale Konfiguration > Logging**

Nachrichten-Log-Einstellungen

Logging aktivieren

☑ Aktionen des UMS Benutzers werden protokolliert.

☐ Aktionen des UMS Benutzers werden nicht protokolliert.

> Protokollmeldungen finden Sie über:
> 1) Menüleiste **> System > Logging > Nachrichten**
> 2) Kontextmenü eines Objekts im Strukturbaum **>** (**Logging**) **> Logging: Nachrichten**

Die folgenden Optionen sind verfügbar, wenn **Logging aktivieren** aktiviert ist:

Logging mit Benutzernamen

☑ Der Name des Administrators, der die Aktion gestartet hat, wird protokolliert.

☐ Der Name wird nicht protokolliert.

Log Level

- Nachrichtentext und -details: Das Protokoll gibt an, welche Aktion an welchem Objekt durchgeführt wurde. Zusätzlich werden weitere Informationen zum Objekt gespeichert.
- Nur Nachrichtentext: Das Protokoll gibt an, welche Aktion an welchem Objekt durchgeführt wurde.

Log Level-Konfiguration: Aktiviert oder deaktiviert die Protokollierung für einzelne Startkommandos. Beispiele: **Profil anlegen**, **View löschen**.

Ereigniseinstellungen aufzeichnen

Ereignisaufzeichnung aktivieren

☑ Von einem Gerät gestartete Aktionen werden protokolliert.

☐ Von einem Gerät gestartete Aktionen werden nicht protokolliert.

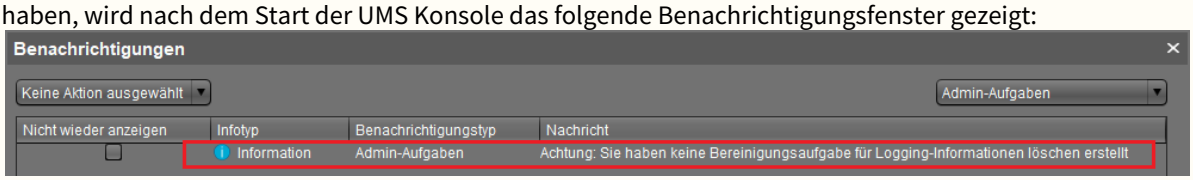
Protokollmeldungen finden Sie über:
1) Menüleiste **> System > Logging > Ereignisse**
2) Kontextmenü eines Objekts im Strukturbaum **>** (**Logging**) **> Logging: Ereignisse**

Die folgende Option ist verfügbar, wenn **Ereignisaufzeichnung aktivieren** aktiviert ist:

Log Level-Konfiguration: Aktiviert oder deaktiviert die Protokollierung für einzelne Startkommandos. Beispiele: **Benutzer authentifizieren**, **Gerät herunterfahren**.

Benachrichtigungen für Admin-Aufgaben

Falls Sie keine administrative Aufgabe für das Löschen von Logging-Informationen (see page 605) angelegt haben, wird nach dem Start der UMS Konsole das folgende Benachrichtigungsfenster gezeigt:



Diese Benachrichtigung können nur Benutzer mit den Leserechten für administrative Aufgaben sehen. Die Rechte können unter **Bearbeiten > Berechtigungen** definiert werden.
Anzeigeeinstellungen können unter **Extras > Einstellungen > Benachrichtigungen** angepasst werden.
Benachrichtigungen sind unter **Hilfe > Benachrichtigungen** zu finden.

Sicherheitsrelevante Ereignisse aufzeichnen

Sicherheitsaufzeihnung aktivieren

☑ Sicherheitsrelevante Ereignisse des ICG, UMS und IMI werden in Dateien protokolliert, die von einem konfigurierten Log Collector (z.B. Graylog) abgeholt werden können. Weitere Informationen finden Sie unter Remote Security Logging for IGEL UMS and ICG (see page 661).

☐ Sicherheitsrelevante Ereignisse des ICG, UMS und IMI werden nicht protokolliert. (Standard)

Dieses Feature loggt persönlich identifizierbare Informationen von UMS-Administratoren, wie z. B. Benutzernamen und IP-Adressen. Stellen Sie sicher, dass Ihre Nutzung dieses Features im Einklang mit den anwendbaren Datenschutzbestimmungen erfolgt, bevor Sie es aktivieren.

Leistungseinstellungen aufzeichnen

Leistungsaufzeichnung aktivieren

☑ Die Überwachung des UMS Servers und, falls vorhanden, des UMS Load Balancers wird gestartet. Die Überwachung liefert statistische Daten und Informationen über die intern aufgerufenen Methoden und deren Parameter, z. B. Anzahl der Aufrufe, Gesamtdauer der Ausführung, usw. Die gesammelten Daten sind vom IGEL Support auszuwerten.
Für die ordnungsgemäße Datenerfassung: Warten Sie nach dem Aktivieren der Leistungsaufzeichnung 3 Minuten und nehmen Sie dann entweder den normalen Betrieb auf oder starten Sie die Aktionen, die Sie überwachen möchten. Nach dem Stoppen der Überwachung warten Sie 5 Minuten, damit das System alle Daten sammeln kann.

Aktivieren Sie die Leistungsaufzeichnung nur nach Rücksprache mit IGEL Support. Die gesammelten Daten können über UMS Konsole > **Hilfe >** Supportinformationen speichern (see page 702) an den IGEL Support gesendet werden.

☐ Die Überwachung ist deaktiviert. (Standard)
Im Falle einer High-Availability (see page 909)-Installation: Wenn die Leistungsaufzeichnung deaktiviert wird, prüfen Sie, dass eine Semaphor-Datei `[Installationsverzeichnis]/umsbroker/etc/conf/statistics.lck`, die vom UMS Load Balancer beim Überwachungsstart erzeugt wird, gelöscht ist.

E-Mail-Einstellungen

Menüpfad: **UMS Administration > Globale Konfiguration > E-Mail-Einstellungen**

Die hier beschriebenen Mail-Einstellungen sind die Voraussetzung für folgende Funktionen:

- View per E-Mail verschicken (see page 515)
- Export der View-Ergebnisse via Mail (see page 515)
- Export der Ergebnisse der folgenden administrativen Aufgaben via E-Mail:
  - Datenbank-Backup (nur für Embedded DB) (see page 599)
  - Unbenutzte Firmwares entfernen (see page 602)
  - Logging-Informationen löschen (see page 605)
  - Ergebnisse von Aufgaben löschen (see page 609)
  - Geräte löschen (see page 618)
  - Einer View Objekte zuordnen (see page 517)
- Mail-Versand der Einmalpasswörter für IGEL Cloud Gateway (ICG)
  Wenn Sie Gmail für das Absenden von Mails verwenden wollen, lesen Sie das How-To E-Mail-Einstellungen für Gmail-Konten (see page 229).
- **SMTP-Host**: Hostnamen oder IP-Adresse des SMTP-Servers (Postausgang)
- **E-Mail-Absenderadresse**: Absenderadresse, die in den E-Mails der UMS erscheinen soll
- **SMTP-Authentifizierung aktivieren**
  ☑ Die UMS meldet sich zum Absenden von Mails beim SMTP-Server an. Die Anmeldedaten müssen unter **SMTP-Benutzername** und **SMTP-Passwort** definiert werden.
- **SMPT-Benutzername**: Benutzername für die Anmeldung beim SMTP-Server
- **SMTP-Passwort**: Passwort für die Anmeldung beim SMTP-Server
- **SMTP-Port**: Port für die Verbindung zwischen der UMS und dem SMTP-Server. Bei unverschlüsseltem SMTP wird standardmäßig Port 25 verwendet, bei SMTP-SSL standardmäßig Port 465, und bei STARTTLS Port 587.
- **SMTP-SSL aktivieren**
  ☑ Die E-Mails werden nach dem Verfahren SMTPS verschlüsselt übertragen.
- **SMTP-STARTTLS aktivieren**
  ☑ Die TLS-Verschlüsselung zum Transport der E-Mails wird nach dem Verfahren STARTTLS eingeleitet.
- **Mögliche TLS Protokolle:** Definiert die Protokolle, die für die Kommunikation mit dem SMTP-Server verwendet werden.

  > ⓘ Wenn kein Protokoll ausgewählt ist, wird TLS 1.0 verwendet. Es muss mindestens ein Protokoll ausgewählt werden. Wenn mehr als ein Protokoll ausgewählt ist, wird die beste Wahl (von links beginnend) verwendet, die vom SMTP-Server akzeptiert wird.

- **Test-Mail senden**: Bei Klick auf diese Schaltfläche schickt die UMS eine Test-Mail. Sie können zwischen zwei Möglichkeiten wählen:
  - Die Test-Mail wird an die E-Mail-Absenderadresse gesendet (Standard)
  - Sende Test-Mail an folgende Adresse
- **Ergebnis**: Zeigt an, ob die Test-Mail erfolgreich abgesendet wurde. Wenn die Mail erfolgreich abgesendet wurde, ist der Text grün hinterlegt, im Fehlerfall rot.

- **E-Mail-Empfänger**: E-Mail-Adressen, an die die Ergebnis-E-Mails zu administrativen Aufgaben sowie die Service-E-Mails gesendet werden. Wenn Sie mehrere Adressen eingeben, müssen Sie diese mit Semikolon ";" voneinander abtrennen.

Nachrichten an Geräte

Menüpfad: **UMS Administration > Globale Konfiguration > Nachrichten an Geräte**

Hier können Sie Templates für Nachrichten an Geräte erstellen, ändern oder entfernen.

Um eine Nachricht zu schreiben, gehen Sie im Kontextmenü des Geräts oder des Geräteverzeichnisses zu **Geräte > Weitere Gerätebefehle > Nachricht senden** oder im Hauptmenü zu **Geräte**. Weitere Informationen finden Sie unter Nachricht senden (see page 474).

Zugelassene Formate für die Nachrichtenübermittlung

Mögliche Optionen:

- "Rich Messages": Die Nachricht kann formatiert werden. Templates können verwendet werden. Allgemein übliche Formate wie Zeichenformate und Schriftgrößen, unnumerierte Listen, Symbole und viele mehr sind verfügbar.
- "Nur reine Textnachrichten": Der Nachrichtentext wird in reinem Text (Plain Text) geschrieben. Es ist möglich, ein Template auszuwählen, aber die Nachricht wird in reinen Text konvertiert.
- "Nachrichtenübermittlung deaktiviert": Das Senden von Nachrichten ist deaktiviert.

Zusätzliche Einstellungen

Menüpfad: **UMS Administration > Globale Konfiguration > Zusätzliche Einstellungen**

Hier finden sich die folgenden globalen Parameter:

Historie der Benutzeranmeldungen

Aktiviere die Historie der Benutzeranmeldungen

☑ Die Aufzeichnung der Anmeldeaktivitäten des Benutzers wird aktiviert. (Standard)

> Ereignisse werden nur protokolliert, wenn der Parameter **Protokolliere Anmelde- und Abmeldeereignisse** unter **System > Fernadministration > Optionen** für das Gerät aktiviert ist (z.B. über Profil).

Füge den jeweils letzten Gerätebenutzer zur Quick Search hinzu

☑ Der zuletzt angemeldete Benutzer wird hinzugefügt.

Füge nur angemeldete Benutzer hinzu

☑ Nur Benutzer, die momentan angemeldet sind, werden hinzugefügt. (Standard)

> Bei Konfigurationsänderungen muss die Seite über  neu geladen werden, damit die Einstellungen übernommen werden.

> Sie können den Benutzerhistorie eines Geräts sowohl in der UMS Konsole als auch in der UMS Web App einsehen:
>
> - UMS Konsole
>   Klicken Sie im Strukturbaum unter **Geräte** das entsprechende Gerät an. Im Inhaltsbereich werden nun alle Informationen rund um das Gerät angezeigt. Wenn Sie ganz nach unten scrollen, können Sie als letzten Punkt die **Historie erfolgreicher Benutzeranmeldungen** aufklappen. Weitere Informationen finden Sie unter Geräteinformationen in der IGEL UMS einsehen (see page 449).
>
> - UMS Web APP
>   Klicken Sie im Strukturbaum unter **Geräte** das entsprechende Gerät an. Alle Informationen über das Gerät werden nun auf der rechten Seite angezeigt. Gehen Sie auf die Registerkarte **Benutzeranmeldungshistorie**, um die Benutzeranmeldungsinformationen zu sehen. Weitere Informationen finden Sie unter Geräte - Ihre Endgeräte in der IGEL UMS Web App ansehen und verwalten (see page 799).

Benachrichtigungen

Benachrichtigungen aktivieren

☑ Benachrichtigungen sind aktiviert und werden bei jeder neuen Verbindung mit der UMS Konsole angezeigt; siehe auch die Einstellungen unter **Menüleiste > Extras > Einstellungen > Benachrichtigungen**. (Standard) Detaillierte Informationen zu Benachrichtigungen finden Sie unter Benachrichtigungen in der IGEL UMS konfigurieren (see page 221).

☐ Die Benachrichtigungsfunktion ist für alle Benutzer deaktiviert.

Für jede Lizenz, jedes Zertifikat und jedes Product Pack wird eine neue Benachrichtigung [...] Tag(e) vor Ablauf erstellt: Setzt eine Frist für eine Warnung, um Sie an den Ablauf Ihrer Lizenz, Ihres Zertifikats oder Product Packs zu erinnern.

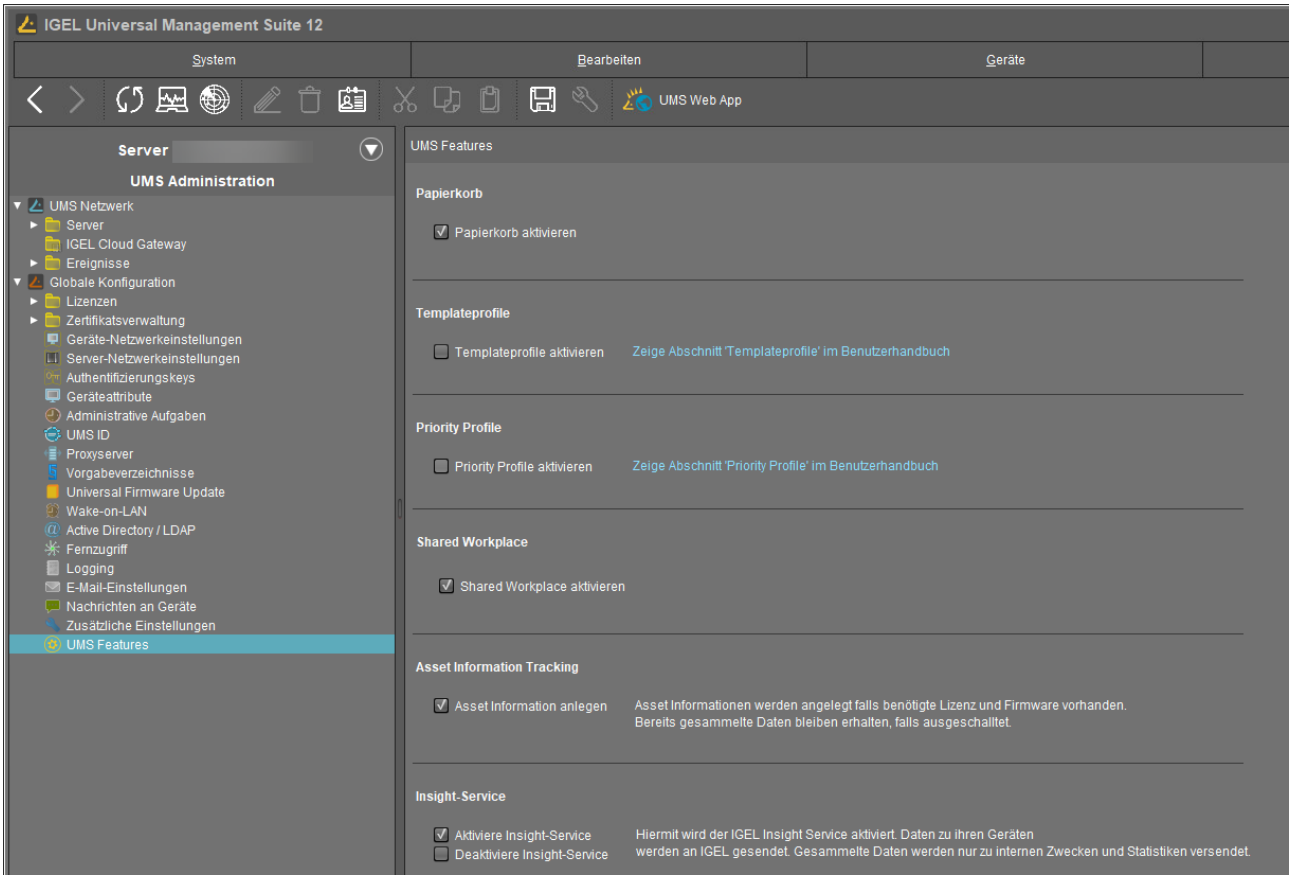
Erstelle Warnungen, wenn der freie Speicherplatz unterhalb von [...] GB liegt: Wenn der freie Speicherplatz unter dem angegebenen Wert liegt, wird eine Warnung erstellt.

Für jede Lizenz und jedes Product Pack wird eine neue Benachrichtigung erstellt, wenn die Anzahl an genutzten Lizenzen unter [...] % fällt: Wenn die Anzahl der genutzten Lizenzen in einem Product Pack höher ist als dieses Limit (ganzzahliger Prozentwert), wird eine Warnung erzeugt.

UMS Features

In der IGEL Universal Management Suite (UMS) können Sie Features wie Papierkorb, Templateprofile oder Priority Profile, IGEL Shared Workplace, usw. aktivieren / deaktivieren.

Menüpfad: **UMS Konsole > UMS Administration > Globale Konfiguration > UMS Features**



Papierkorb

Papierkorb aktivieren

☑ Der Papierkorb wird aktiviert. Wird ein Objekt im Strukturbaum gelöscht, so wird es in den Papierkorb verschoben. (Standard)

> ⓘ Wenn der Papierkorb deaktiviert ist, werden die Objekte sofort dauerhaft gelöscht.

Siehe auch Papierkorb - Löschen von Objekten in der IGEL UMS (see page 545).

Templateprofile

Templateprofile aktivieren

☑ Templateprofile werden aktiviert. Informationen zu Templateprofilen finden Sie unter Templateprofile in der IGEL UMS (see page 416).

☐ Templateprofile werden deaktiviert. (Standard)

Priority Profile

Priority Profile aktivieren

☑ Priority Profile werden aktiviert. Informationen zu Priority Profilen finden Sie unter Priority Profile in der IGEL UMS (see page 413).

☐ Priority Profile werden deaktiviert. (Standard)

Shared Workplace

Shared Workplace aktivieren

☑ IGEL Shared Workplace (SWP) (see page 488) wird aktiviert. (Standard)

Lizenziertes Feature

Für dieses Feature ist eine gültige Lizenz aus dem Enterprise Management Pack (EMP) erforderlich.

Bei der Deaktivierung von **Shared Workplace aktivieren** wird der Strukturbaumknoten **Shared Workplace-Benutzer** ausgeblendet. Die Benutzer von Shared Workplace können sich dann NICHT mehr anmelden!

Asset Information Tracking

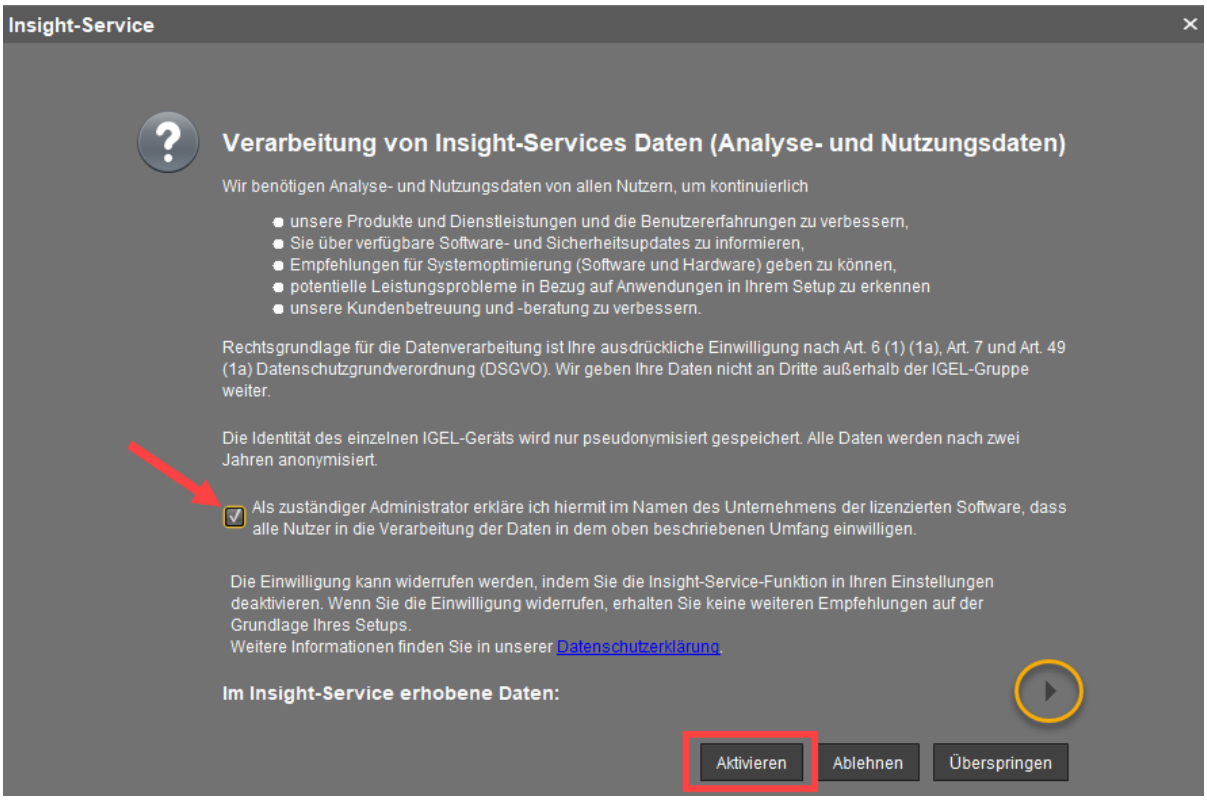
Asset Information anlegen

☑ Das Asset Information Tracking (see page 452) ist aktiviert. (Standard)

Insight Service

Aktiviere Insight Service

☑ Aktiviert den IGEL Insight Service, wenn Sie die Datenschutzrichtlinien in dem geöffneten Dialog akzeptieren und auf **Aktivieren** klicken. Wenn Sie den IGEL Insight Service aktivieren, sammelt IGEL spezifische Analyse- und Nutzungsdaten; siehe IGEL Insight Service.



Deaktiviere Insight Service

☑ Deaktiviert den IGEL Insight Service, wenn Sie in dem geöffneten Dialog auf **Ablehnen** klicken.

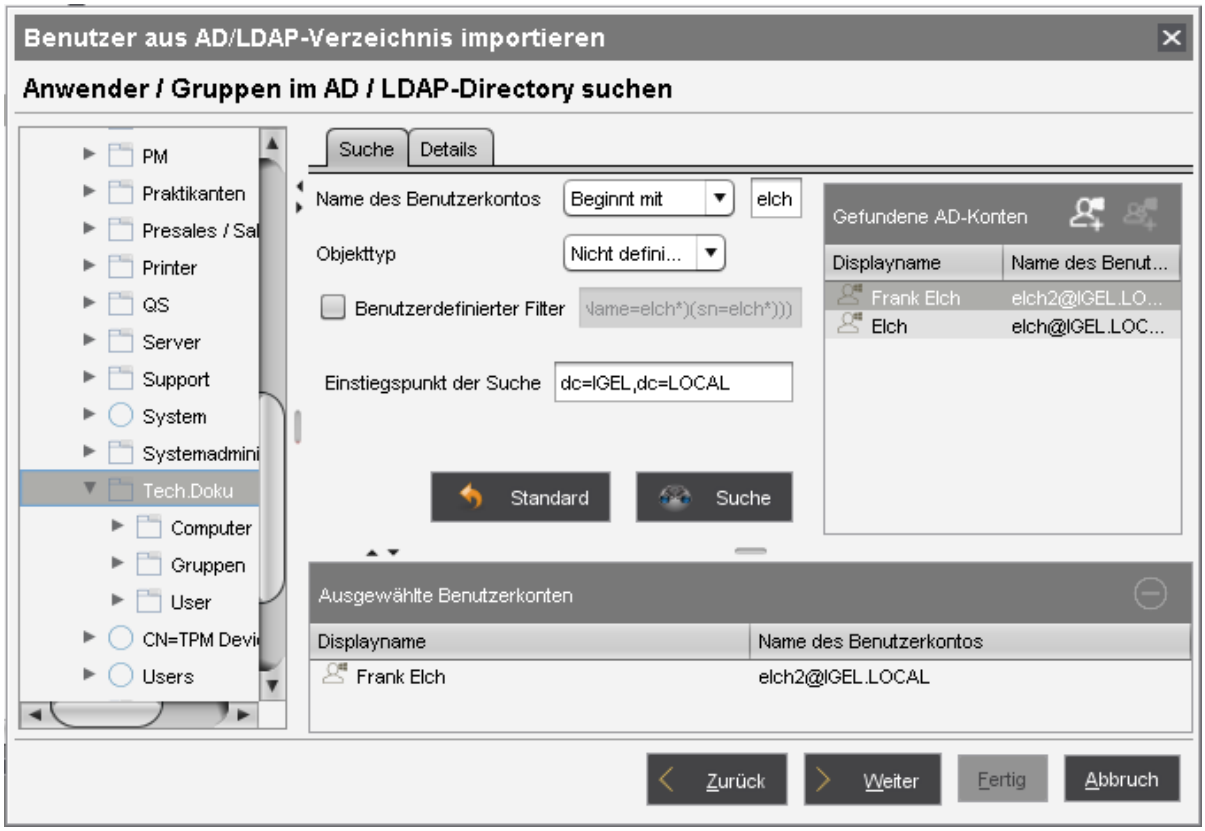
Active Directory Benutzer importieren

Der Import von Benutzern aus dem Active Directory in die UMS Konsole erfolgt in drei Schritten:

- Anmeldung am Active Directory
- Auswahl der zu importierenden Benutzer und Start des Imports
- Protokoll des Importprozesses

So importieren Sie Benutzer aus dem Active Directory in die UMS Konsole:

1. Starten Sie den Importdialog der UMS Konsole über **System > Administratorkonten > Importieren**.
2. Melden Sie sich am AD/LDAP-Service an.
   Die Anbindung ist unter Active Directory / LDAP einbinden (see page 657) beschrieben. Nur angebundene ADs stehen zur Auswahl für den Import von Benutzerkonten.
3. Klicken Sie **Weiter**.
   Es öffnet sich der Active Directory-Browser.
4. Wählen Sie einzelne Benutzer oder Gruppen aus dem Navigationsbaum Ihres ADs aus.
   Die markierten Benutzer/Gruppen lassen sich über das Kontextmenü oder per Drag-and-Drop in die zu importierende Auswahl übernehmen bzw. wieder entfernen. Aus der Trefferliste **Gefundene AD Accounts** lassen sich die gefundenen Benutzer/Gruppen über die Symbole in die Liste **Ausgewählte Accounts** übertragen.
   Eine Mehrfachauswahl verschiedener Benutzer und Gruppen ist möglich.



Alternativ zur Navigation im Navigationsbaum lassen sich Benutzer oder Gruppen auch über die **Suche** selektieren und der Auswahl hinzufügen.

5. Klicken Sie **Weiter** um den Import zu starten.
   Ein Bestätigungsfenster öffnet sich.

Der erfolgreiche Import eines Benutzers kann nicht rückgängig gemacht werden, Sie müssen den irrtümlich angelegten UMS Administrator in der Verwaltung der Administratorkonten manuell löschen. Als Name des importierten AD-Benutzers wird in der *IGEL* UMS das **Konto** verwendet.

Suche im Active Directory

Im AD-Navigationsbaum haben die Optionen folgende Bedeutung:

Name des Benutzerkontos: Suche basierend auf Kontonamen bzw. Teilen davon

Objekttyp: Suche auf Benutzer oder Gruppen beschränken

Benutzerdefinierter Filter: Filterkriterien entsprechend des RFC-2254-Standards

Einstiegspunkt der Suche	Startelement im Baum, an welchem die Suche beginnt
Standard	Setzt alle Suchoptionen auf die Standardwerte
Suche	Startet die eingestellte Suche

Das Kontextmenü erlaubt folgende Aktionen auf Elemente der Trefferliste:

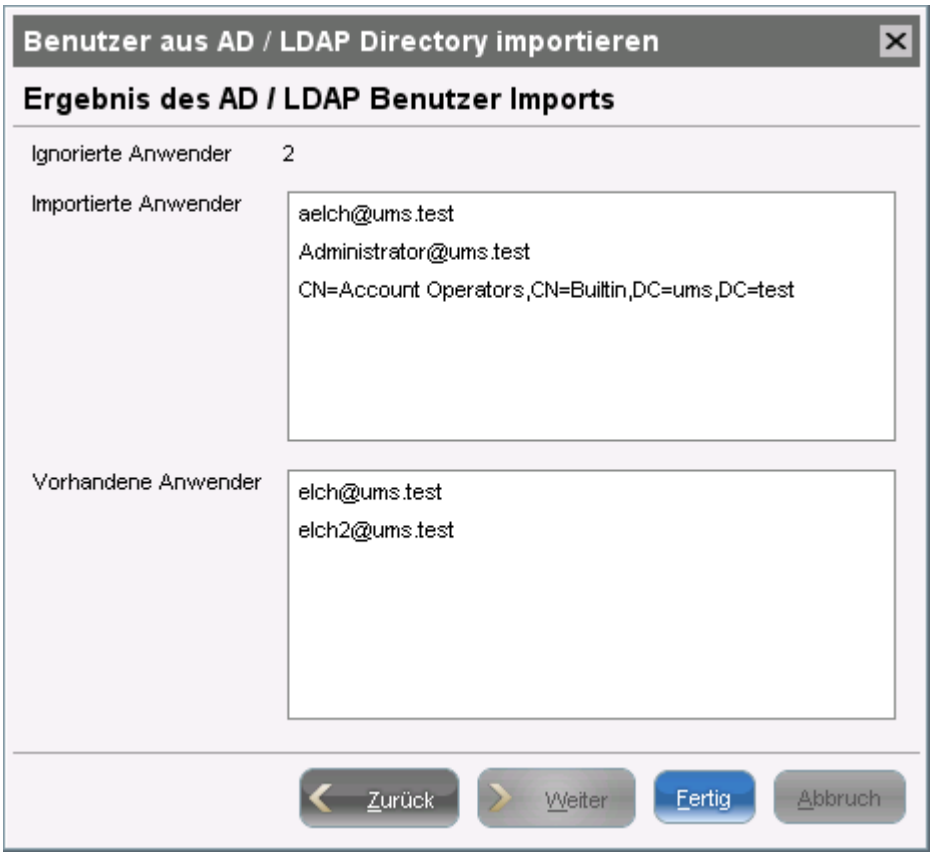
- **Anwender hinzufügen**
- **Gruppe hinzufügen**
- **Einstiegspunkt der Suche festlegen**
- **Details...**

Unter **Details** können Sie sich die Eigenschaften der für den Import ausgewählten Objekte nochmals anzeigen lassen und eventuell Objekte vor dem Import entfernen.

Ergebnisliste des Imports

Im Anschluss an den Import öffnet sich ein Ergebnisfenster.

Hier wird angezeigt, wie viele Konten beim Import ignoriert wurden und welche Konten erfolgreich importiert wurden. Ist ein Benutzerkonto in der UMS bereits vorhanden, wird dieses AD-Konto beim Import übersprungen.



Administratorkonten und Zugriffsrechte

Menüpfad: Menüleiste **> System > Administratorkonten**

Für die Anmeldung an der UMS Konsole / UMS Web App (see page 238) können Sie UMS Administratorkonten entweder aus einem angebundenen Active Directory importieren oder aber auch manuell erstellen, organisieren und entfernen.

An diesen Administratorkonten bzw. -gruppen hängen die Zugriffsrechte auf Objekte oder Aktionen innerhalb der IGEL UMS. Die Rechte des während der Installation erstellten UMS Superusers (siehe IGEL UMS unter Linux installieren (see page 253) oder IGEL UMS unter Windows installieren (see page 266)) können nicht eingeschränkt werden. Der UMS superuser hat immer volle Zugriffsrechte in der UMS.

UMS Web App

Die UMS Web App unterstützt die gleichen Berechtigungen wie die UMS Konsole. Um Zugriff auf Geräte in einem Verzeichnis zu erhalten, sind Leseberechtigungen für dieses Verzeichnis erforderlich; Berechtigungen nur für Geräte sind nicht ausreichend.
Weitere Informationen zu Berechtigungen in der UMS Web App finden Sie unter Wichtige Informationen zur IGEL UMS Web App (see page 784).

Administratoren und Gruppen

Menüpfad: Menüleiste **> System > Administratorkonten**

▶ Klicken Sie in der Menüleiste **System > Administratorkonten**, um die IGEL UMS Administratorkonten zu verwalten.

Alle vorhandenen Konten sind in der linken Spalte gelistet, die vorhandenen Gruppen in der rechten. Rechts der jeweiligen Spalte finden Sie die zugehörigen Schaltflächen wie **Neu**, **Bearbeiten**, **Entfernen**. Für Administratorkonten können Sie zudem das Passwort ändern (**Passwort ändern**) und die Gruppenmitgliedschaft anzeigen (**Mitglied von**). Die Schaltfläche **Mitglieder** zeigt Details zu den Mitgliedern einer gewählten Gruppe. Über **Effektive Rechte** haben Sie Einblick in die Rechte, die einem Benutzer direkt oder indirekt zugewiesen oder ihm entzogenen wurden.

Zugriffsrechte

Berechtigungen in der IGEL UMS umfassen:

- allgemeine Rechte, die einem Administrator direkt über das Konto oder indirekt über die Gruppenzugehörigkeit zugewiesen bzw. verweigert werden können
- Zugriffsrechte auf Objekte im Strukturbaum
- Zugriffsrechte auf Knoten im Administrationsbereich der UMS Konsole

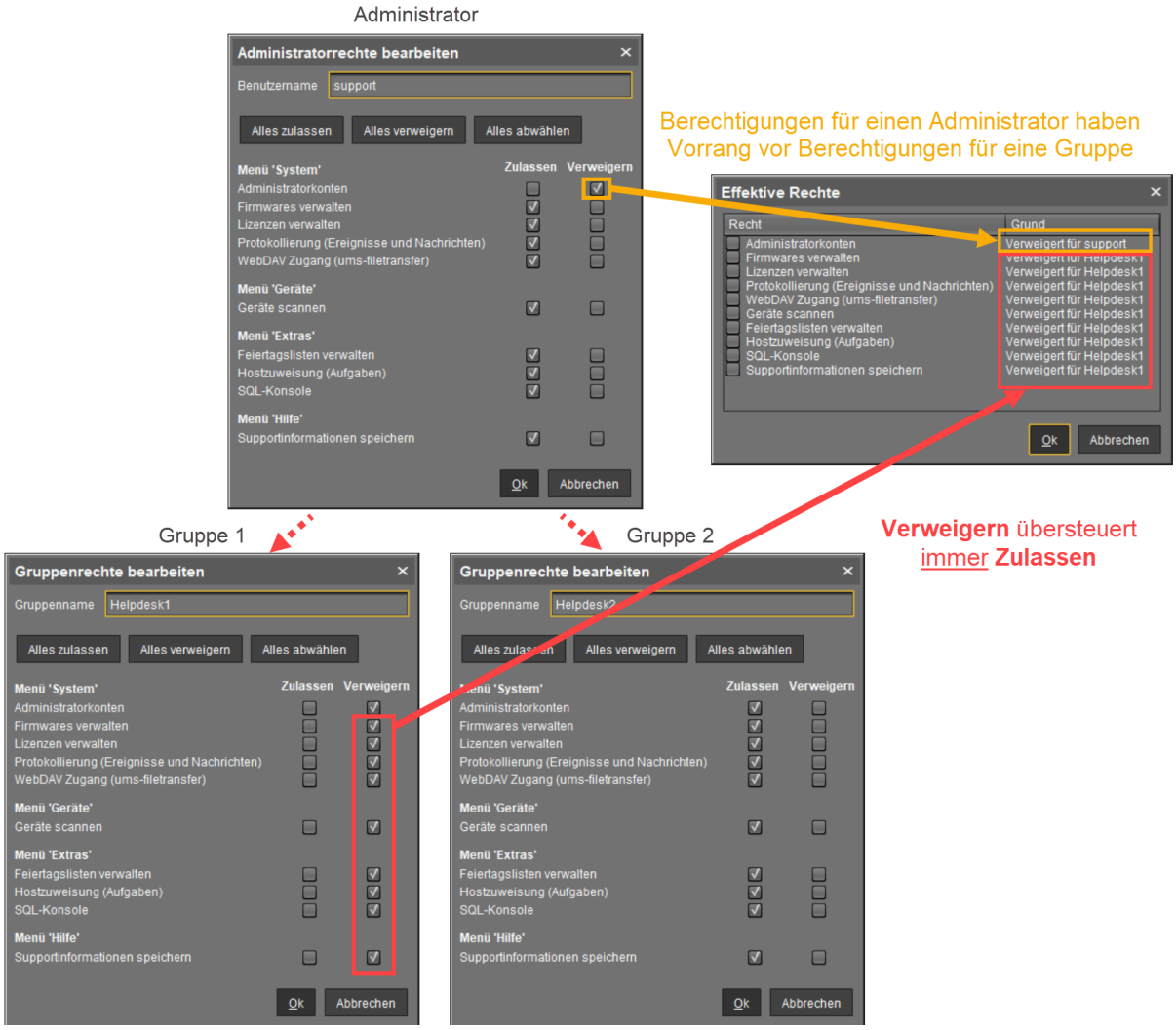
Die indirekten Rechte, die ein Administrator über seine Gruppenzuweisung erhält, lassen sich für jeden Administrator der Gruppe weiter ändern.

⚠ Beachten Sie:
- Die direkt zugewiesenen Rechte haben Vorrang vor den indirekt zugewiesenen Rechten.
- Allerdings hat der Entzug einer Berechtigung IMMER Vorrang gegenüber der Gewährung.

Der Vorrang des Rechts **Verweigern** vor dem Recht **Zulassen** bedeutet:

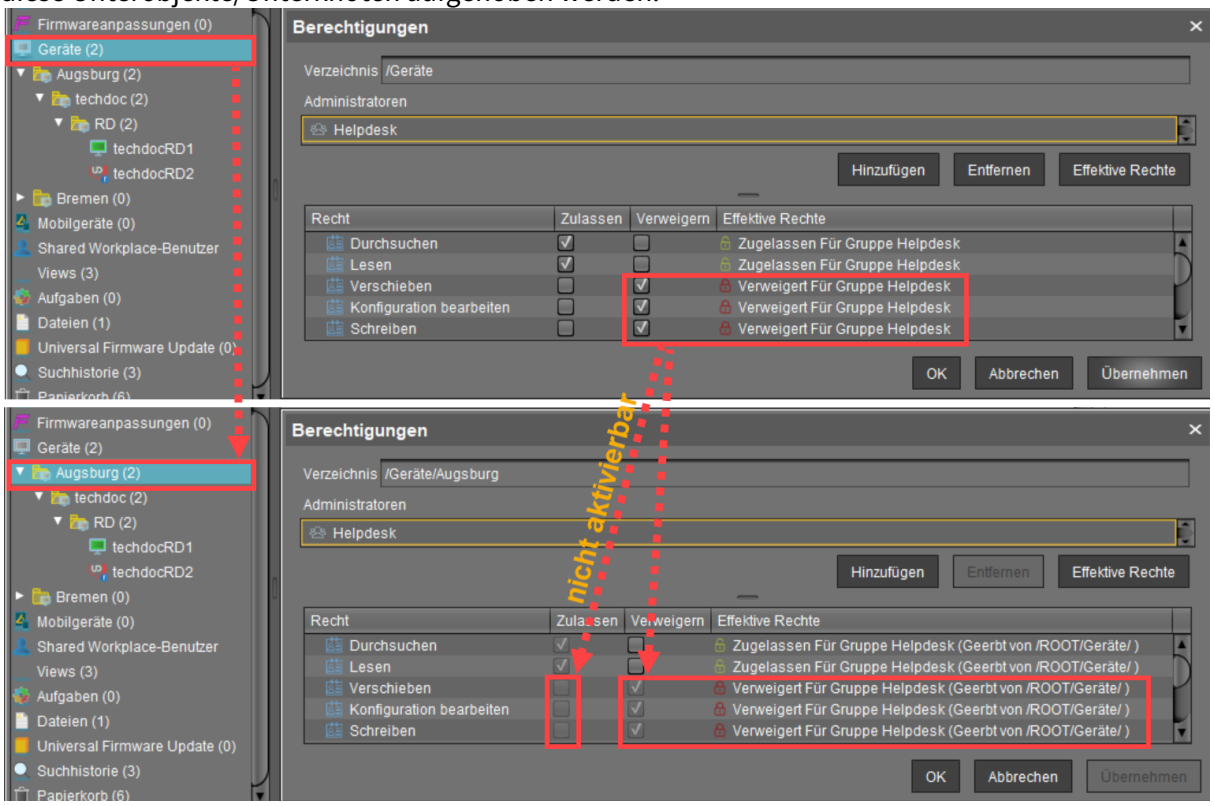
- Wenn ein Administrator Mitglied mehrerer Gruppen ist, deren Berechtigungen einander widersprechen, wird die Berechtigung **Verweigern** die Berechtigung **Zulassen** aus anderen Gruppen übersteuern. Auch wenn die Berechtigung einem Administrator direkt erteilt wird, wird

sie dennoch über eine Gruppe verweigert.



- Wenn ein Verbot für ein Objekt im Strukturbaum oder einen Knoten im Bereich UMS Administration erlassen wird, gilt es für alle Unterobjekte/Unterknoten und kann nicht direkt für

diese Unterobjekte/Unterknoten aufgehoben werden.



Generell werden für Gruppen wie für Administratoren die gleichen Berechtigungseinstellungen vorgenommen. Die folgende Beschreibung einzelner Konfigurationsmöglichkeiten gilt daher sowohl für Administratoren als auch für Gruppen.

- Grundlegende Berechtigungen (see page 681)
- Allgemeine Administratorenrechte (see page 682)
- Objektbezogene Zugriffsrechte (see page 687)
- Zugriffsrechte im Administrationsbereich (see page 693)

Grundlegende Berechtigungen

In der nachfolgenden Tabelle sind die grundlegenden Zugriffsrechte gelistet, die zum Anlegen, Bearbeiten oder Löschen von Objekten benötigt werden. Ein Objekt ist z. B. ein Verzeichnis, Element des Strukturbaums (Geräte, Profile…) oder auch Knoten im Administrationsbereich der UMS Konsole, etwa administrative Aufgaben oder die AD-Anbindung.

Aktion	Betroffene Objekte	Durchsuchen	Lesen	Verschieben	Konf. Bearbeiten	Schreiben	Berechtigungen
Allgemein							
Objekt anzeigen	Baumelement (Profil, Thin Client...)		X				
	Verzeichnis	X					
Objekt anlegen	Zielverzeichnis					X	
Objekt löschen	Objekt					X	
	Quellverzeichnis					X	
Objekt bearbeiten	Objekt					X	
Objekt umbenennen	Objekt					X	
Konfiguration anzeigen	Thin Client, Profil		X				
Konfiguration bearbeiten	Thin Client				X		
	Profil					X	
Effektive Rechte anzeigen	Objekt		X				
	Verzeichnis	X					
Berechtigung ändern	Objekt, Verzeichnis						X
Import	Zielverzeichnis					X	

Allgemeine Administratorenrechte

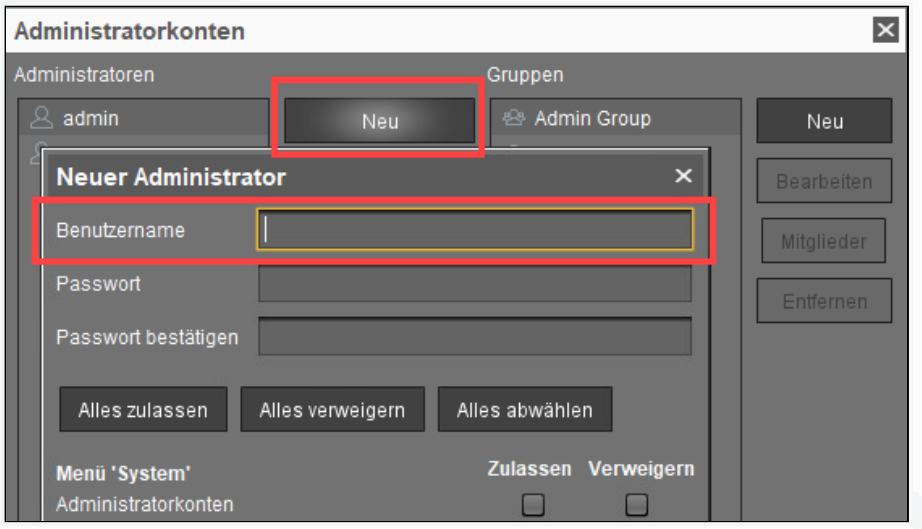
Menüpfad: Menüleiste **> System > Administratorkonten**

Über **System > Administratorkonten** werden die Berechtigungen gesteuert. Ein Administrator kann für sich und andere Rechte gewähren und entziehen sowie neue Konten anlegen.

Folgende Optionen stehen Ihnen hier nach Administratoren oder Gruppen aufgeteilt zu Verfügung:

Neu: Ein neuer Administrator oder eine neue Gruppe wird angelegt.

Die folgenden Zeichen sind für Benutzernamen von UMS Administratoren nicht erlaubt: `"/ \ [ ] : ; | = , + * ? < >`



Importieren: Ein Benutzer wird aus dem AD/LDAP-Verzeichnis importiert.

Dieser Vorgang benötigt eine AD/LDAP-Verbindung. Zu weiteren Details siehe Active Directory Benutzer importieren (see page 672).

- **Domäne**: Domäne, in der der AD/LDAP Service läuft
- **Benutzer**: Name des Benutzers
- **Passwort**: Passwort des Benutzers

Bearbeiten: Vorhandene Administratoren- oder Gruppeneinstellungen können bearbeitet werden.

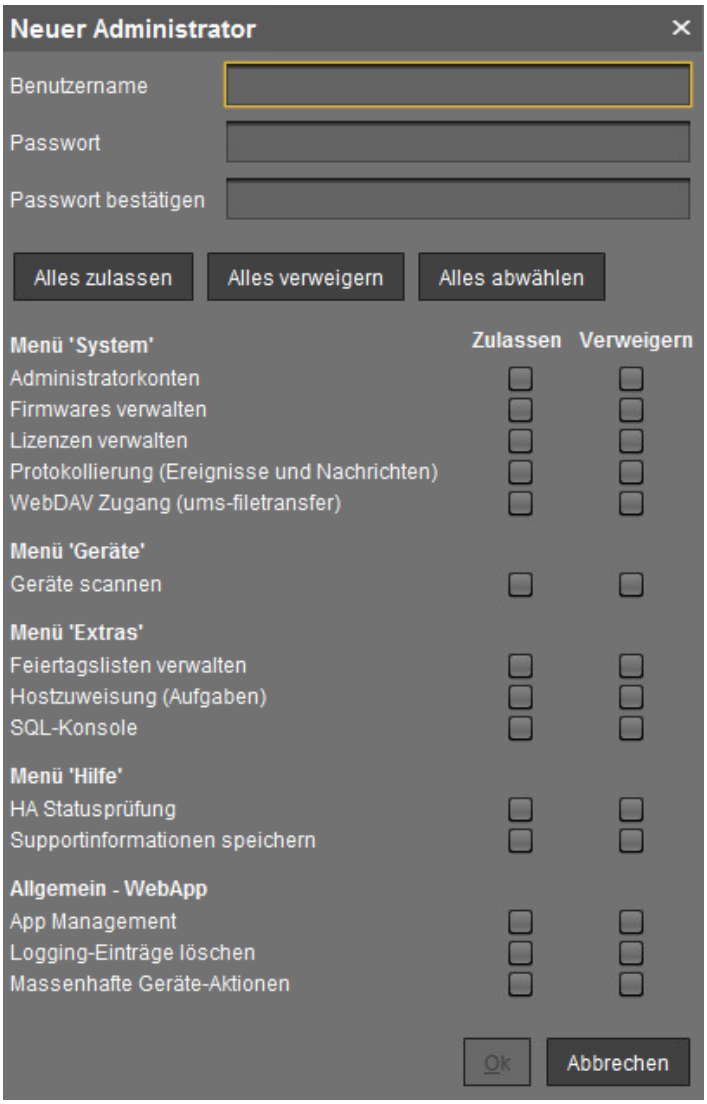
Effektive Rechte: Eine Liste aller zugewiesener Rechte zu einem bestimmten Administrator wird angezeigt.

Mitglied von / Mitglieder: Die Zuordnung von Mitgliedschaften und Gruppen wird angezeigt.

Passwort ändern: Ändern eines Administratorpasswortes

Entfernen: Entfernen eines markierten Administrators oder einer Gruppe

Im Folgenden finden Sie eine Liste mit Berechtigungen, die einzelnen Administratoren oder Gruppen unter **System > Administratorkonten > Neu** oder **Bearbeiten** vergeben werden können. Jede Berechtigung hat drei mögliche Zustände: nicht gesetzt, **Zulassen** oder **Verweigern**.



Menü 'System'

Administratorkonten

☑ Die Berechtigungsverwaltung darf ausgeführt werden: Administratoren und Gruppen sowie ihre Rechte können hinzugefügt und bearbeitet werden.

Die Berechtigung **Administratorkonten** sollte nur Benutzern gewährt werden, die generell Zugriff auf alle Objekte und Aktionen in der UMS erhalten sollen!

Firmwares verwalten

☑ Firmwareversionen können importiert, exportiert und aus der Datenbank entfernt werden.

Lizenzen verwalten

☑ IGEL Firmwarelizenzen können an Geräte vergeben werden.

Protokollierung (Ereignisse und Nachrichten)

☑ Einsicht in das Ereignis- und Nachrichten-Log ist zugelassen, wenn **Logging** aktiv ist.

WebDAV Zugang (ums-filetransfer)

☑ Der Benutzer hat die Berechtigung, Dateien im Verzeichnis `/ums_filetransfer/` hinzuzufügen, zu ändern und zu löschen.

Menü 'Geräte'

Geräte scannen

☑ Es kann nach Geräten im Netzwerk gescannt werden, um diese z. B. am UMS Server zu registrieren.

Menü 'Extras'

Feiertagslisten verwalten

☑ Feiertage können für die Planung von Aufgaben definiert werden.

Hostzuweisung (Aufgaben)

☑ Geplante Aufgaben können verschiedenen Hosts zugewiesen werden.

SQL-Konsole

☑ Die SQL-Konsole darf ausgeführt werden. **Vorsicht:** Die SQL-Konsole kann der Datenbank erheblichen Schaden zufügen.

Menü 'Hilfe'

HA Statusprüfung

☑ Die Funktion UMS HA Statusprüfung - Ihre High Availability- und Distributed UMS-Systeme analysieren (see page 944) für eine Gesamtprüfung der High-Availability-Umgebung kann verwendet werden.

Supportinformationen speichern

☑ Datenbank- und Server-Logdateien können für Supportzwecke exportiert werden.

Allgemein - WebApp

App Management

☑ Der Bereich **Apps** der UMS Web App wird angezeigt. Der Benutzer ist berechtigt, Apps zu verwalten.

Logging-Einträge löschen

☑ Protokollnachrichten können mit der UMS Web App gelöscht werden.

Massenhafte Geräte-Aktionen

☑ Aktionen können für eine beliebige Anzahl von Geräten mit der UMS Web App durchgeführt werden.

☐ Aktionen können mit der UMS Web App nur für jeweils ein Gerät durchgeführt werden.

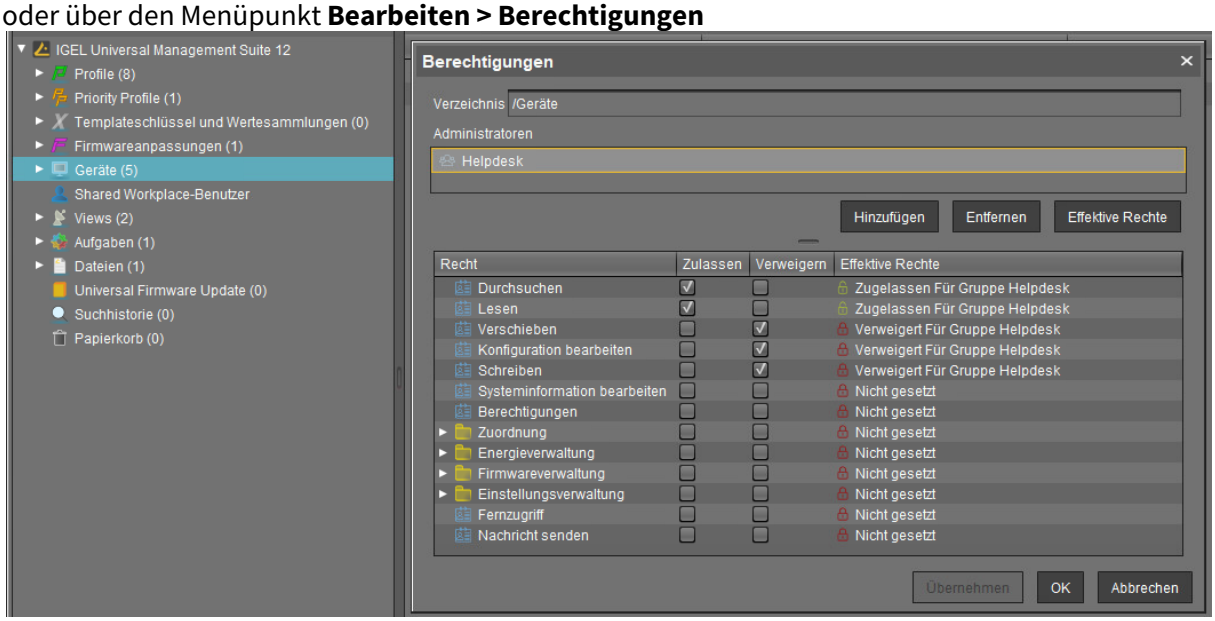
⚠ Dies gilt nur für die UMS Web App; mit der UMS Konsole können weiterhin massenhafte Aktionen durchgeführt werden.

Objektbezogene Zugriffsrechte

Administratoren und Administratorengruppen können bestimmte Rechte an Objekten im Strukturbaum zugewiesen werden. Diese Berechtigungen vererben sich „nach unten", also z. B. von einem Ordner auf die in diesem Ordner liegenden Geräte.

So gelangen Sie nach Auswahl eines Objekts zu den Berechtigungseinstellungen:

- über **Berechtigungen** im Kontextmenü des Objekts
- oder über das Berechtigungssymbol  in der Symbolleiste
- oder über den Menüpunkt **Bearbeiten > Berechtigungen**

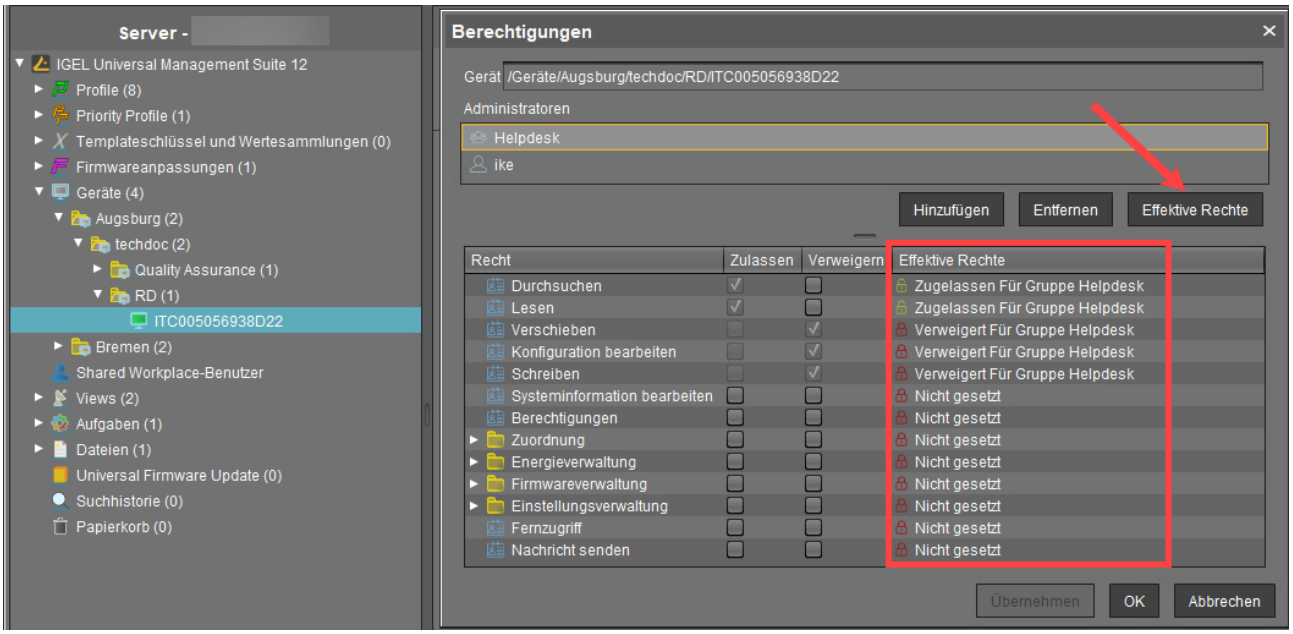


Obige Liste umfasst alle im UMS Strukturbaum verfügbaren objektbezogenen Berechtigungen. Je nach gewähltem Objekt steht davon nur eine Auswahl zur Verfügung. So lassen sich z. B. einer View weder Updates zuordnen, noch kann eine View heruntergefahren werden.

Zusammenhängende Berechtigungen werden automatisch zusammen gesetzt, können aber nachträglich manuell angepasst werden. Aktivierte Berechtigungen oder Verweigerungen auf Knoten betreffen alle Objekte im Knoten.

> ⚠ Der Entzug einer Berechtigung, d.h. **Verweigern**, hat immer Vorrang gegenüber der Gewährung einer Berechtigung, d.h. **Zulassen**.

Die Übersicht zeigt für einen ausgewählten Administrator dessen Rechte am Objekt. Details erhält man über **Effektive Rechte**. Hier werden auch die Regeln der Rechteermittlung angezeigt, z. B. ob eine Berechtigung direkt vergeben wurde oder ob sie über eine Gruppe oder eine Vererbung in der Baumstruktur zugewiesen ist.


Server -
IGEL Universal Management Suite 12
Profile (8)
Priority Profile (1)
Templateschlüssel und Wertesammlungen (0)
Firmwareanpassungen (1)
Geräte (4)
Augsburg (2)
techdoc (2)
Quality Assurance (1)
RD (1)
ITC005056938D22
Bremen (2)
Shared Workplace-Benutzer
Views (2)
Aufgaben (1)
Dateien (1)
Universal Firmware Update (0)
Suchhistorie (0)
Papierkorb (0)
Berechtigungen
Gerät /Geräte/Augsburg/techdoc/RD/ITC005056938D22
Administratoren
Helpdesk
ike
Hinzufügen
Entfernen
Effektive Rechte
Recht
Zulassen
Verweigern
Effektive Rechte
Durchsuchen
Zugelassen Für Gruppe Helpdesk
Lesen
Zugelassen Für Gruppe Helpdesk
Verschieben
Verweigert Für Gruppe Helpdesk
Konfiguration bearbeiten
Verweigert Für Gruppe Helpdesk
Schreiben
Verweigert Für Gruppe Helpdesk
Systeminformation bearbeiten
Nicht gesetzt
Berechtigungen
Nicht gesetzt
Zuordnung
Nicht gesetzt
Energieverwaltung
Nicht gesetzt
Firmwareverwaltung
Nicht gesetzt
Einstellungsverwaltung
Nicht gesetzt
Fernzugriff
Nicht gesetzt
Nachricht senden
Nicht gesetzt
Übernehmen
OK
Abbrechen

Verfügbare Rechte

Allgemein	**Durchsuchen**	Sichtbarkeit des Objekts im Strukturbaum (Pfad bis zum Objekt muss ebenfalls erlaubt werden!)
	Lesen	Leserecht auf Ordnerinhalte bzw. Objekteigenschaften
	Verschieben	Geräte dürfen ohne Schreibrecht verschoben werden.
	Konfiguration bearbeiten	Schreibrecht für die Konfiguration eines Geräts (Setup)
	Schreiben	Schreibrecht auf Ordner bzw. Objekteigenschaften (nicht Setup)
	Systeminformation bearbeiten	Die Systeminformationen eines Geräts (Geräteattribute) können bearbeitet werden.
	Berechtigungen	Die Berechtigungseinstellungen des Objekts dürfen geändert werden.
	Fernzugriff	VNC- / Sicheres Terminal-Zugriff auf den Geräten
	Nachricht senden	Nachrichten können an Geräte gesendet werden.
Zuordnung	**(Priority) Profil zuordnen**	Dem Objekt darf ein Profil zugeordnet werden. Diese Berechtigung ist für die Zuweisung von Apps für IGEL OS 12-Geräte erforderlich.
	Datei zuordnen	Dem Objekt darf eine Datei zugeordnet werden.
	Basissystem / Firmwareupdate zuordnen	Dem Objekt darf eine IGEL OS Base System App / ein Firmwareupdate zugeordnet werden.
	FWC zuordnen	Dem Objekt darf eine Firmwareanpassung zugeordnet werden.
	Templateschlüssel / Wertesammlung zuordnen	Dem Objekt darf ein Templateschlüssel / eine Wertesammlung zugeordnet werden.
Energieverwaltung	**Neustart**	Das Gerät neu starten.
	Standbymodus	Das Gerät in den Standbymodus versetzen.

	Herunterfahren	Das Gerät herunterfahren.
	Wakeup	Das Gerät per Wake-on-LAN aufwecken.
Firmwareverwaltung	**Update**	Das App- / Firmwareupdate darf durchgeführt werden.
	Zurücksetzen	Die Firmware auf Werkseinstellungen zurücksetzen.
	Flash Player	Das Flash-Player-Plugin für Firefox herunterladen.
	Filetransfer	Eine zugewiesene Datei darf zum Gerät übertragen werden.
	Generic Command	Generische Befehle (z. B. spezifische Gerätebefehle wie Installiere Jabra Xpress Paket) können an das Gerät gesendet werden.
Einstellungsverwaltung	**UMS -> Gerät**	Die Konfiguration der UMS kann an das Gerät gesendet werden.
	Gerät -> UMS	Die lokale Konfiguration des Geräts kann in die UMS eingelesen werden.

Objekte zuordnen

Die Zuordnung von Objekten erfordert folgende Berechtigungen:

- **Durchsuchen**
- **Lesen**
- **Zuordnen** auf beiden Seiten

> **Schreibrechte** sind für die unmittelbare Zuordnung von Objekten nicht erforderlich.

Beispiel 1: Eine Datei einem Profil zuweisen

Ein Benutzer kann eine Datei nur einem Profil zuordnen oder diese Zuordnung löschen. Er kann an der Datei oder dem Profil keine Änderungen vornehmen, d. h. er kann sie nicht bearbeiten, umbenennen oder löschen.

Berechtigungen für das Profil

Recht	Zulassen	Verweigern	Effektive Rechte
Durchsuchen	☑	☐	Zugelassen Für Benutzer ike (Geerbt von /ROOT/Profile/)
Lesen	☑	☐	Zugelassen Für Benutzer ike (Geerbt von /ROOT/Profile/)
Schreiben	☐	☐	Nicht gesetzt
Berechtigungen	☐	☐	Nicht gesetzt
▼ Zuordnung	☐	☐	Nicht gesetzt
Datei zuordnen	☑	☐	Zugelassen Für Benutzer ike
Gerät zuordnen	☐	☐	Nicht gesetzt
Shared Workplace...	☐	☐	Nicht gesetzt

Berechtigungen für die Datei

Recht	Zulass...	Verweig...	Effektive Rechte
Durchsuchen	☑	☐	Zugelassen Für Benutzer ike (Geerbt von /ROOT/Datei...
Lesen	☑	☐	Zugelassen Für Benutzer ike (Geerbt von /ROOT/Datei...
Schreiben	☐	☐	Nicht gesetzt
Berechtigungen	☐	☐	Nicht gesetzt
▼ Zuordnung	☐	☐	Nicht gesetzt
Profil zuordnen	☑	☐	Zugelassen Für Benutzer ike
Priority Profil zuordnen	☐	☐	Nicht gesetzt
FWC zuordnen	☐	☐	Nicht gesetzt
Gerät zuordnen	☐	☐	Nicht gesetzt

Beispiel 2: Ein Gerät einem Profil zuweisen

Ein Benutzer kann ein Gerät nur einem Profil zuordnen oder diese Zuordnung löschen. Er kann an dem Gerät oder Profil keine Änderungen vornehmen, d. h. er kann das Gerät oder Profil nicht umbenennen, löschen oder deren Konfiguration bearbeiten.

Berechtigungen für das Profil

Recht	Zulassen	Verweigern	Effektive Rechte
Durchsuchen	☑	☐	Zugelassen Für Benutzer ike (Geerbt von /ROOT/Profile/)
Lesen	☑	☐	Zugelassen Für Benutzer ike (Geerbt von /ROOT/Profile/)
Schreiben	☐	☐	Nicht gesetzt
Berechtigungen	☐	☐	Nicht gesetzt
▼ Zuordnung	☐	☐	Nicht gesetzt
Datei zuordnen	☐	☐	Nicht gesetzt
Gerät zuordnen	☑	☐	Zugelassen Für Benutzer ike
Shared Workplace...	☐	☐	Nicht gesetzt

Berechtigungen für das Gerät

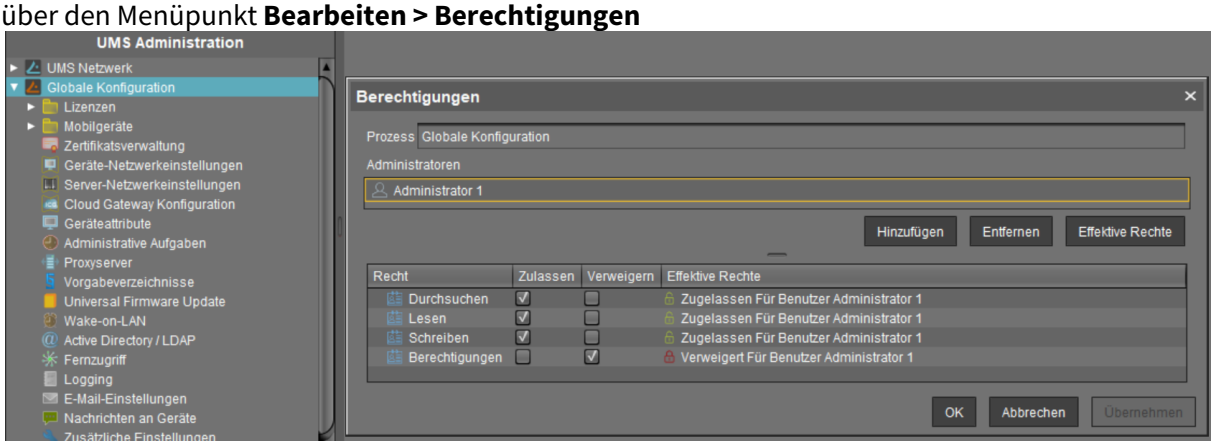
Recht	Zulassen	Verweigern	Effektive Rechte
Durchsuchen	☑	☐	Zugelassen Für Benutzer ike (Geerbt von /ROOT/G...
Lesen	☑	☐	Zugelassen Für Benutzer ike (Geerbt von /ROOT/G...
Verschieben	☐	☐	Nicht gesetzt
Konfiguration bearbeiten	☐	☐	Nicht gesetzt
Schreiben	☐	☐	Nicht gesetzt
Systeminformation bearbeiten	☐	☐	Nicht gesetzt
Berechtigungen	☐	☐	Nicht gesetzt
▼ Zuordnung	☐	☐	Nicht gesetzt
Profil zuordnen	☑	☐	Zugelassen Für Benutzer ike
Priority Profil zuordnen	☐	☐	Nicht gesetzt
Datei zuordnen	☐	☐	Nicht gesetzt
Basissystem / Firmwareup...	☐	☐	Nicht gesetzt
FWC zuordnen	☐	☐	Nicht gesetzt
Templateschlüssel / Werte...	☐	☐	Nicht gesetzt
▶ Energieverwaltung	☐	☐	Nicht gesetzt
▶ Firmwareverwaltung	☐	☐	Nicht gesetzt
▼ Einstellungsverwaltung	☑	☐	Zugelassen Für Benutzer ike
UMS -> Gerät	☑	☐	Zugelassen Für Benutzer ike
Gerät -> UMS	☑	☐	Zugelassen Für Benutzer ike
Fernzugriff	☐	☐	Nicht gesetzt
Nachricht senden	☑	☐	Zugelassen Für Benutzer ike

Zugriffsrechte im Administrationsbereich

Im Bereich **UMS Administration** können Sie die allgemeinen Rechte **Durchsuchen**, **Lesen**, **Schreiben**, **Berechtigungen** für Administratorkonten vergeben bzw. verweigern. Berechtigungen sollten nur an Benutzer vergeben werden, die tatsächlich administrative Aufgaben an der UMS ausführen sollen.

So gelangen Sie nach Auswahl eines Baumknotens zu den Berechtigungseinstellungen:

- über **Berechtigungen** im Kontextmenü
- über das Berechtigungssymbol  in der Symbolleiste
- über den Menüpunkt **Bearbeiten > Berechtigungen**



Benutzeraktionen protokollieren

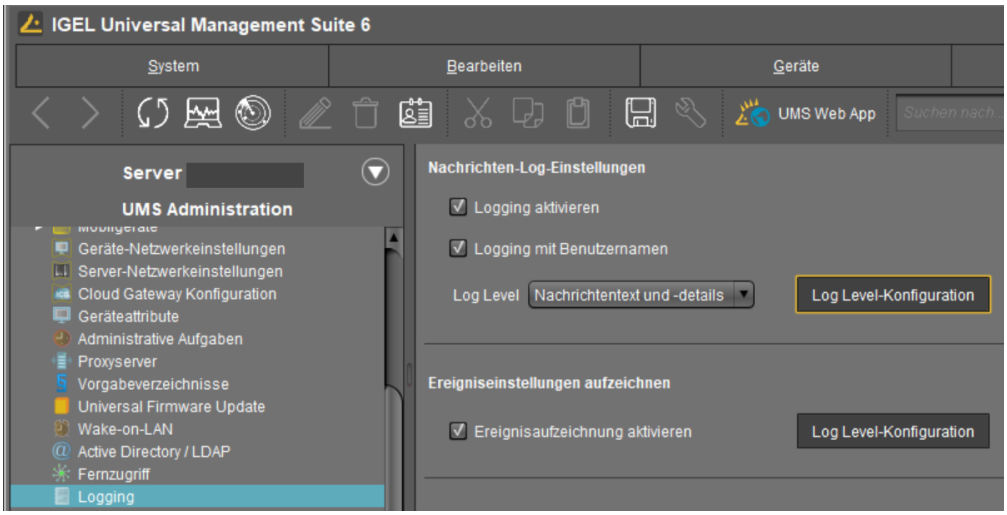
Das Protokollsystem wird von der UMS und das registrierten Gerät verwendet, um alle Datenbankänderungen aufzuzeichnen. Nur erfolgreiche Aktionen werden protokolliert. Fehler finden Sie in der Protokolldatei des UMS GUI-Servers nicht.

Das Protokollsystem ist in zwei Bereiche unterteilt:

Messages (Nachrichten):	Von einem Benutzer gestartete Aktionen
Events (Ereignisse):	Von einem Gerät gestartete Aktionen

Administration

Die Administrationseinstellungen für den Protokollierungsvorgang werden in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Logging** konfiguriert, siehe Logging (see page 661).



- **Nachrichten** können entweder mit oder ohne Details protokolliert werden.
  Für **Ereignisse** gibt es keine Details.
- Mit den **Log-Level-Konfiguration**-Schaltflächen aktivieren Sie die Protokollierung für ausgewählte Befehle. Standardmäßig ist die Protokollierung für alle möglichen Befehle ausgewählt.
- Das Löschen und der Export von Protokollen werden unter **UMS Administration > Globale Konfiguration > Administrative Aufgaben** konfiguriert.

Protokolle anzeigen

Meldungen zu **Nachrichten** und **Ereignisse** lassen sich in der UMS Konsole folgendermaßen anzeigen:

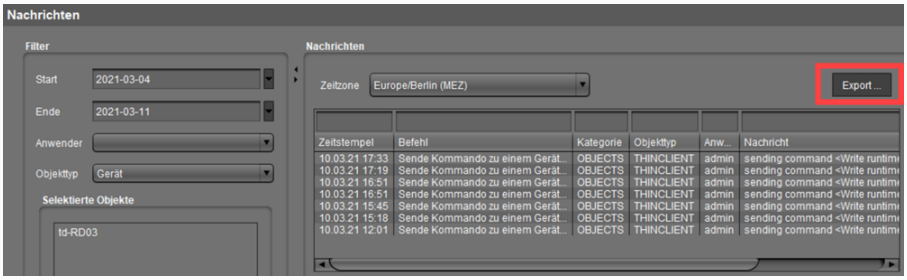
- über das Menü **System > Logging**
- über **Logging** im Kontextmenü der Verzeichnisse und Objekte im Strukturbaum

- Dialogfenster Logging: Filter einstellen (see page 696)

Dialogfenster Logging: Filter einstellen

So stellen Sie einen Filter ein:

1. Geben Sie Im Fensterbereich **Filter** Kriterien an, um selektive Nachrichten aus der Datenbank zu laden.
   Alle Filterfelder werden mit dem Operator **AND** kombiniert.
   Nur wenn die Mehrfachauswahl für ein Filterfeld möglich ist, werden diese Werte mit dem Operator **OR** verbunden, z. B. wenn mehrere Geräte ausgewählt werden.
2. Klicken Sie auf **Filter anwenden**, um die neuen Einstellungen zu aktivieren.
   Die Protokollnachrichten oder -ereignisse werden aus der Datenbank entsprechend den Filtereinstellungen neu geladen.

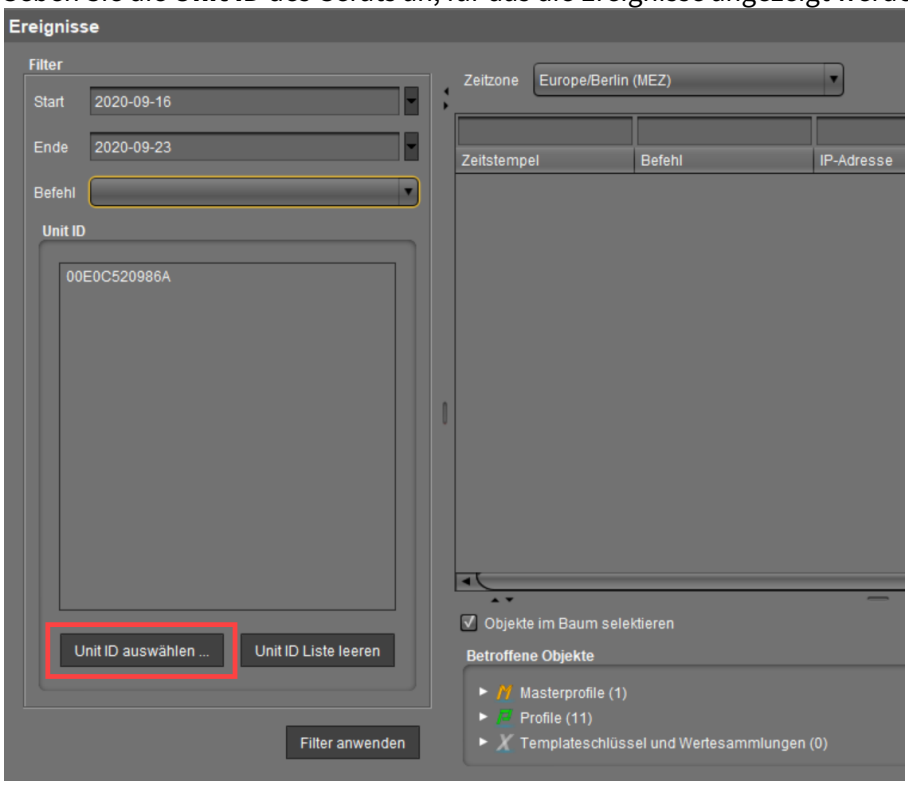
> **Nachrichten/Ereignisse** können mit **Export** in HTML-, XML- und CSV-Dateien exportiert werden.
>
> 
>

- Filter für Ereignisse einstellen (see page 697)
- Filter für Nachrichten (see page 698)
- Filter für Kategorien einstellen (see page 699)
- Anmerkungen (see page 700)

Filter für Ereignisse einstellen

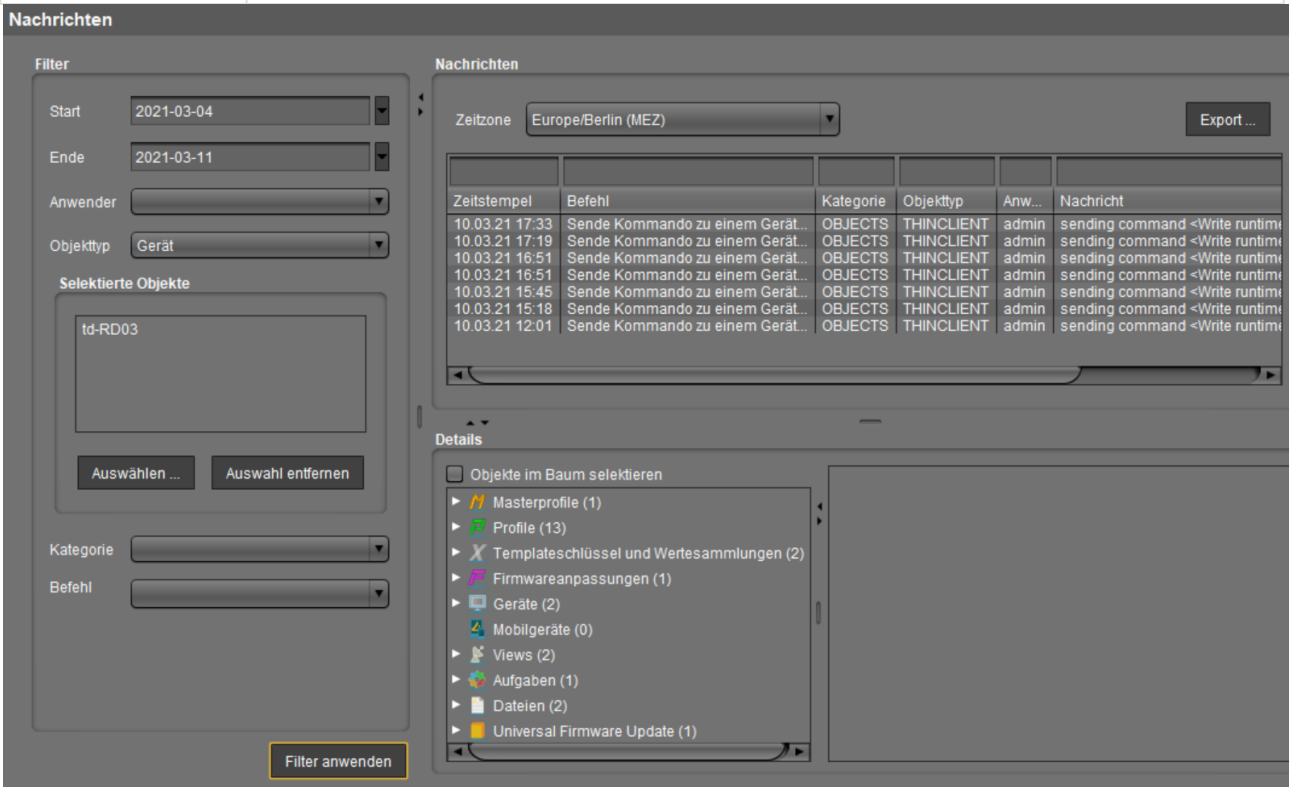
So stellen Sie den Filter für Ereignisse ein:

1. Geben Sie den **Befehl** an, wenn er Ihnen bekannt ist.
2. Geben Sie die **Unit ID** des Geräts an, für das die Ereignisse angezeigt werden sollen.



Filter für Nachrichten

Anwender	Wählen Sie den Namen des UMS Administrators aus, der für die Nachricht zuständig ist.
Objekttyp	Geben Sie ein Objekt an, für das Sie die Nachrichten anzeigen lassen möchten.
Kategorie	Jeder Befehl gehört einer Kategorie an, z. B. Sicherheit, Einstellungen und Objekte.
Befehl	Wenn ein Kommando bekannt ist, können Sie dieses selbst angeben.
Zeitzone	Sie können die Zeitzone angeben, mit der die Protokollzeit der Nachrichten angezeigt wird.



Filter für Kategorien einstellen

▶ Wählen Sie für die Anpassung des Filters die Option **Kategorie**, wenn Sie alle Nachrichten für eine bestimmte Kategorie (wie z. B. zu Firmware Updates) auswählen möchten.
Alle Kommandos dieser Kategorie wie **Firmware Update löschen** oder **Firmware Update zuweisen** werden für die Ermittlung der Nachrichten oder Ereignisse ausgewertet.

Anmerkungen

Der Schnellfilter gilt nicht für die Exportaktion.

Einer der wichtigsten Befehle ist der Befehl `GET_SETTINGS_ON_REBOOT`. Über den Zeitstempel dieses Befehls erhalten Sie die letzte Startzeit auf dem Gerät. Diese kann verwendet werden, um ein neues **BOOTTIME-**View-Kriterium zu definieren. Mit diesem Kriterium können Sie alle Geräte ganz einfach ermitteln, die nach einem bestimmten Datum noch nicht gestartet worden sind.

> Die Administrationseinstellungen für die Menge der Nachrichten und - noch wichtiger - für die Ereignisse sollten mit großer Sorgfalt gehandhabt werden. Je höher diese Werte sind, umso mehr Platz wird für den Tablespace in der Datenbank benötigt. Wenn Sie die Protokollierung aktivieren, sollten Sie Ihre Datenbank genau beobachten, bis Sie sich sicher sind, dass in der Datenbank ausreichend Platz für die Nachrichten und/oder Ereignisse verfügbar ist.

Supportinformationen speichern / Logdateien an den Support senden

Falls Sie Probleme mit der UMS haben und Ihren Serviceanbieter kontaktieren, können Sie verschiedene Logdateien der UMS an den Support senden. Hierbei hilft Ihnen der Support-Assistent in der IGEL UMS (see page 702).

Bei Fragen rund um das IGEL Produkt wenden Sie sich bitte zunächst an den für Sie zuständigen Vertriebspartner, sofern Sie bereits IGEL Kunde sind.

Wenn Sie zur Zeit IGEL Produkte testen, oder falls Sie von Ihrem Vertriebspartner die gewünschte Hilfe nicht bekommen können, füllen Sie bitte nach dem Einloggen auf dem IGEL Customer Portal[32] das Supportformular aus.

Wir werden Sie umgehend unterstützen. Sie erleichtern die Arbeit unserer Supportmitarbeiter, wenn Sie uns möglichst alle verfügbaren Informationen zukommen lassen. Bitte beachten Sie hierzu auch unsere Hinweise zu Support- und Serviceauskünften[33].

32 https://cosmos.igel.com/
33 https://www.igel.com/terms-conditions/

Support-Assistent in der IGEL UMS

Mit dem Support-Assistenten können Sie die für Ihren Supportfall wichtigen Logdateien sammeln und als E-Mail an den IGEL Support senden.

Der Support-Assistent speichert Logdateien von UMS Server und UMS Konsole sowie Profile und zugehörige Firmware-Informationen der ausgewählten Geräte in einer ZIP-Datei. Falls IGEL Cloud Gateway (ICG) verwendet wird, werden auch alle Logdateien der verbunden ICGs sowie die grundlegenden Informationen der verwendeten ICG-Zertifikate gespeichert. Ist die Erweiterung IGEL Management Interface (IMI) im Einsatz, wird auch deren API-Logdatei mit gespeichert. Im Falle der Leistungsaufzeichnung (nur nach Rücksprache mit IGEL Support zu aktivieren; siehe Logging (see page 662)) werden auch Überwachungsdaten für den UMS Server und den UMS Load Balancer gesammelt.

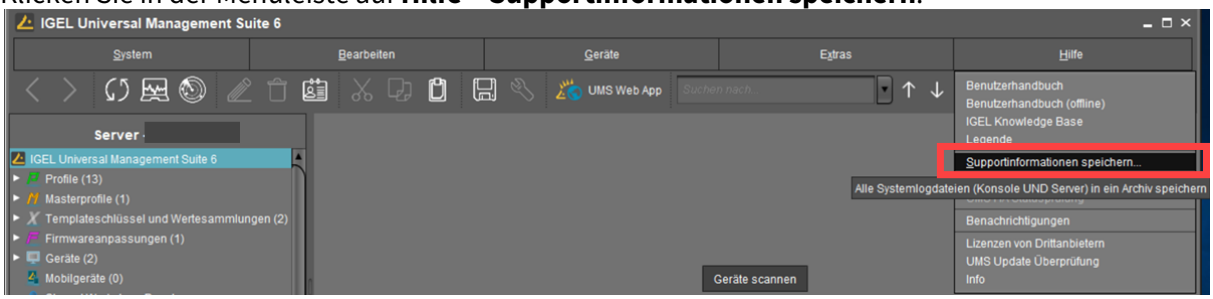
Menüpfad: **Menüleiste > Hilfe > Supportinformationen speichern**

> Um Logdateien mit dem Support-Assistenten zu versenden, müssen die E-Mail-Einstellungen korrekt sein; weitere Informationen finden Sie unter E-Mail-Einstellungen (see page 664). Außerdem muss die Support-ID gültig sein.

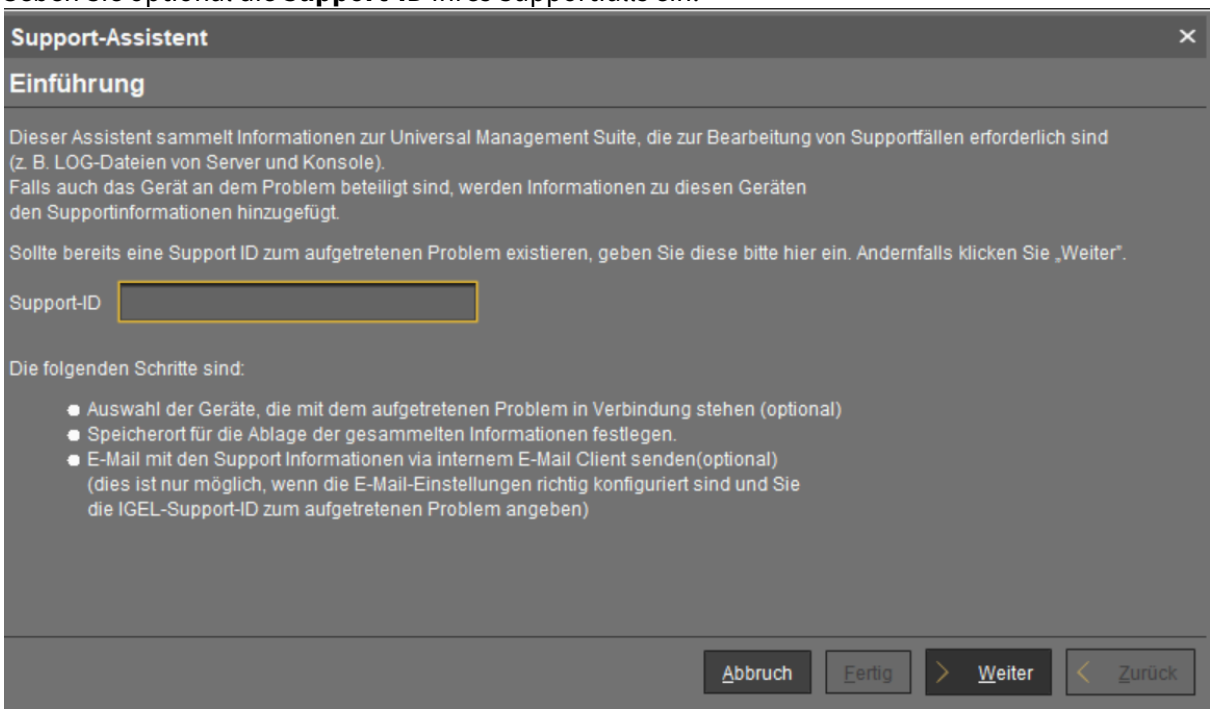
Protokolldateien über den Support-Assistenten in der IGEL UMS versenden

So versenden Sie Logdateien mit dem Support-Assistenten:

1. Klicken Sie in der Menüleiste auf **Hilfe > Supportinformationen speichern**.



2. Geben Sie optional die **Support-ID** Ihres Supportfalls ein.



3. Klicken Sie **Weiter**.
4. Falls der Supportfall Geräte betrifft (andernfalls klicken Sie **Weiter**): Markieren Sie die Geräte, bei denen das Problem aufgetreten ist.
5. Falls der Supportfall Geräte betrifft (andernfalls klicken Sie **Weiter**): Selektieren Sie mit  die markierten Geräte.
6. Klicken Sie **Weiter**.
7. Geben Sie unter **Tage zurück** an, wie viele Tage die versendenden Logeinträge höchstens zurückliegen sollen.
8. Klicken Sie **Weiter**.
9. Wählen Sie mit **Suchen in** das Verzeichnis in Ihrem Dateisystem aus, in dem die gezippte Logdateien gespeichert werden sollen.
10. Klicken Sie **Weiter**.

> ⓘ Wenn die gezippten Logdateien bereits gespeichert wurden, werden Sie gefragt, ob die vorhandene ZIP-Datei überschrieben werden soll.

Wenn die E-Mail-Einstellungen konfiguriert sind, werden Eingabefelder für die E-Mail angezeigt. Wenn die E-Mail-Einstellungen nicht konfiguriert sind, wird eine Medlung über die gespeicherten Dateien angezeigt.

11. Falls anwendbar, geben Sie die folgenden Informationen für die E-Mail ein:
    - **Cc**: E-Mail-Adresse, an die eine Kopie gesendet werden soll. Wenn Sie mehrere Adressen eingeben, müssen Sie diese mit Semikolon ";" voneinander abtrennen.
    - **Antwortadresse**: E-Mail-Adresse, an die die Antwort vom Support gesendet werden soll. Wenn Sie das Feld leer lassen, wird die Antwort an die unter **UMS Administration > E-Mail-Einstellungen** definierte **E-Mail-Absenderadresse** gesendet.
    - **Betreff**: Betreff der E-Mail. Beim Absenden wird diesem Text die **Support-ID** vorangestellt.
    - Texteingabefeld: Text der E-Mail.

12. Überprüfen Sie die Informationen für die E-Mail und klicken Sie **Senden**.

13. Klicken Sie **Fertig**.

Ähnliche Themen

Debugging / How to Collect Log Files

Lokale Gerätekonfiguration exportieren

Gerätedateien für den Support speichern

Sie können die IGEL Universal Management Suite (UMS) verwenden, um Protokolldateien von einem Gerät zu speichern. Diese Protokolldateien werden gezippt, so dass Sie sie einfach zum IGEL Support-Team senden können. Das genaue Verhalten hängt von der Firmware-Version des Geräts ab.

Menüpfad: **Menüleiste > Hilfe > Gerätedateien für den Support speichern**

Protokolldateien eines Geräts speichern

1. Gehen Sie zu **Hilfe > Gerätedateien für den Support speichern**.
   Ein Assistent öffnet sich. Auf der Seite **Gerät auswählen** wird der Gerätebereich des Strukturbaums angezeigt.
2. Wählen Sie das Gerät aus, dessen Protokolldateien Sie speichern wollen, und klicken Sie **Weiter**.
   Die Seite **Zielordner für die gezippten Dateien wählen** wird angezeigt.
3. Wählen Sie einen Zielordner und klicken Sie **Weiter**.
   Die Protokolldateien werden vom Gerät geholt und gezippt. Der Dateipfad wird angezeigt.
4. Klicken Sie **Fertig**.

Eine detaillierte Anleitung mit Screenshots finden Sie unter Debugging / How to Collect and Send Device Log Files to IGEL Support.

Sammeln der Protokolldateien von IGEL OS 11 Geräte

Standardmäßig werden die folgenden Protokolldateien gesammelt:

- `/config/Xserver/card0`
- `/config/Xserver/monitor-info`
- `/config/Xserver/xorg.conf-0`
- `/config/sound/card0`
- `/config/sound/default_card_name`
- `/var/log/Xorg.0.log`
- `/wfs/group.ini`
- `/wfs/setup.ini`
- dhclient lease files

Im IGEL Setup können Sie unter **Zubehör > Systemprotokolle > Optionen** weitere Protokolldateien hinzufügen. Weitere Informationen finden Sie unter Options.

Sammeln der Protokolldateien von IGEL OS 12 Geräte

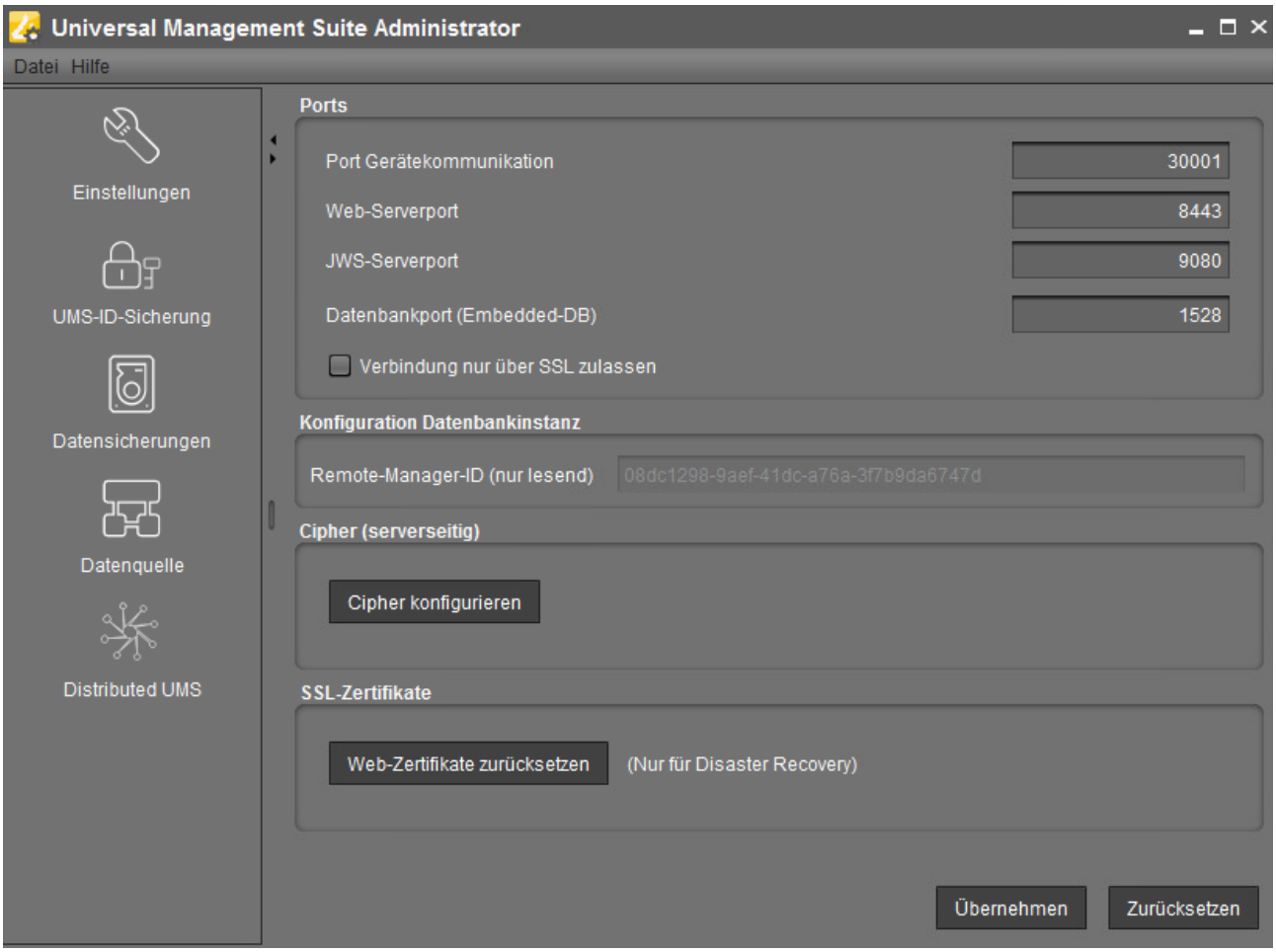
Standardmäßig werden die folgenden Protokolldateien gesammelt:

- `/config/Xserver/card0`
- `/config/Xserver/monitor-info`
- `/config/Xserver/xorg.conf-0`
- `/var/log/Xorg.0.log`
- `/var/log/auth.log`
- `/var/log/daemon.log`
- `/var/log/igfmount.log`
- `/var/log/kern.log`
- `/var/log/syslog`
- `/var/log/tcsetup.log`
- `/wfs/user/setup-assistant.log`

Im IGEL Setup können Sie unter **Zubehör > Systemprotokolle** weitere Protokolldateien hinzufügen lokal auf dem Gerät oder über die UMS Web App. Weitere Informationen finden Sie unter System Log Viewer.

Der IGEL UMS Administrator

Die Anwendung IGEL UMS Administrator ist ausschließlich auf einem UMS Server verfügbar, da sie Ihnen ermöglicht, die Kommunikation zwischen den Diensten direkt zu ändern. Mit ihr lassen sich z.B. Grundeinstellungen wie zu verwendende Ports oder angebundene Datenquellen bearbeiten. Diese Funktionen stehen im Administrationsbereich der UMS Konsole nicht zur Verfügung.



Lässt sich der UMS Administrator unter Linux nicht per Menü- oder Desktopverknüpfung starten, können Sie die Anwendung auf der Kommandozeile mit folgendem Befehl starten: `/ [IGEL Installationsverzeichnis]/RMAdmin.sh` (wenn das standardmäßige Installationsverzeichnis verwendet wird: `/opt/IGEL/RemoteManager/RMAdmin.sh`)
Es wird NICHT empfohlen, `RMAdmin.sh` als `sudo` auszuführen. Unter Red Hat Enterprise Linux 8 kann der Befehl `RMAdmin.sh` nur ohne `sudo` ausgeführt werden.

Der Standardpfad zum UMS Administrator unter Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`

Unter **Datei > Einstellungen > Sprache** können Sie die Sprache des Administratortools ändern.

Die Berechtigungen für die Änderung von Einstellungen sind davon abhängig, ob eine Berechtigung für die Änderung der IGEL UMS Dateien auf dem Serversystem besteht. Sie sollten daher für die Verwendung des IGEL UMS Administrators dasselbe Benutzerkonto verwenden, mit dem Sie die Installation der UMS durchgeführt haben.

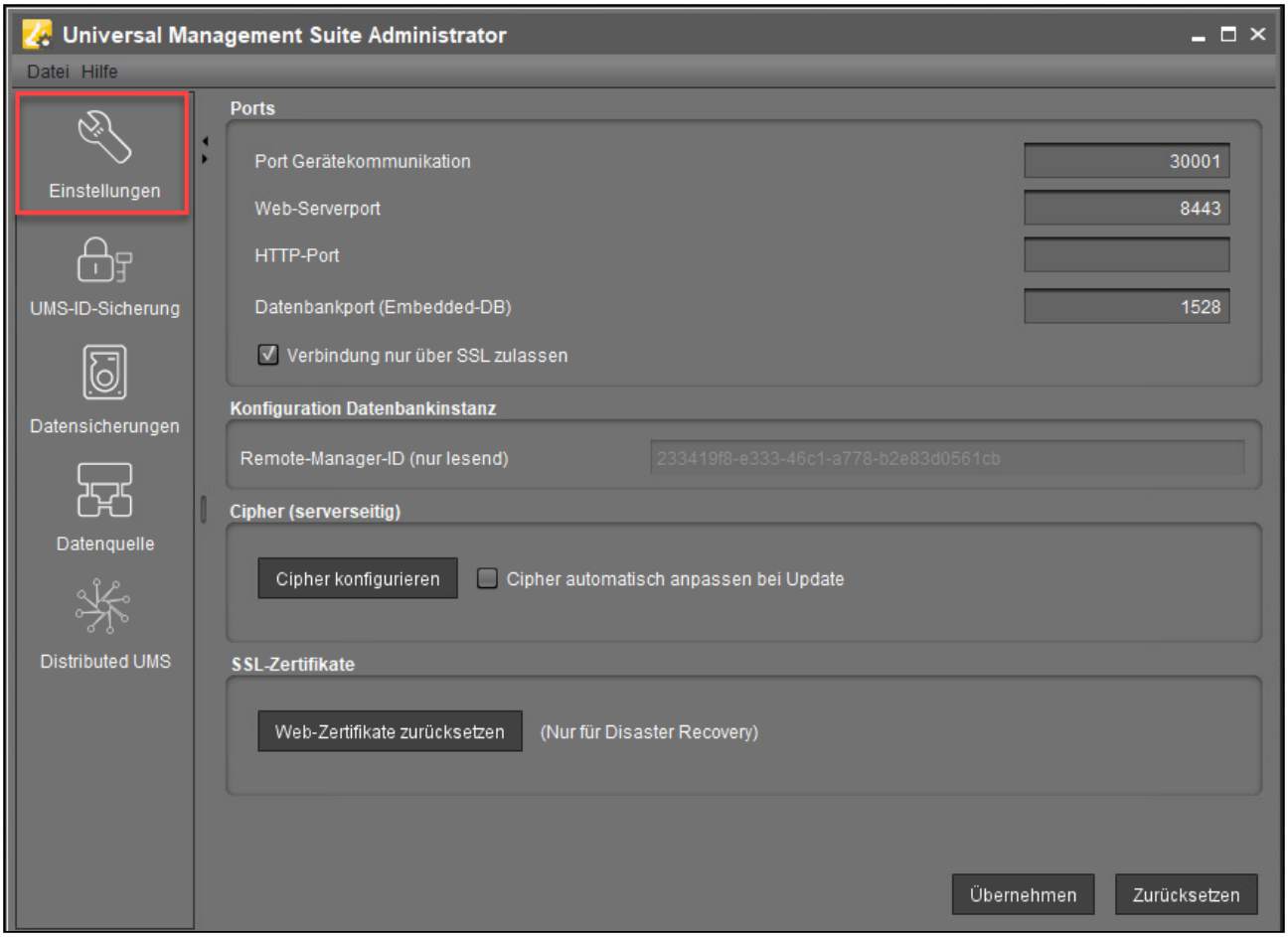
- Einstellungen - Servereinstellungen im IGEL UMS Administrator ändern (see page 709)
- UMS-ID-Sicherung im IGEL Administrator (see page 713)
- Datensicherungen (see page 719)
- Datenquelle (see page 729)
- Distributed UMS - Lokale UMS-Aktionen im IGEL UMS Administrator ausführen (see page 738)
- IGEL UMS Administrator Kommandozeilenschnittstelle (see page 740)

Einstellungen - Servereinstellungen im IGEL UMS Administrator ändern

Mit dem IGEL Universal Management Suite (UMS) Administrator können Sie verschiedene Servereinstellungen editieren, z.B. Web-Server-Port, Cipher, usw.

> Standardpfad zum UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

Menüpfad: **UMS Administrator > Einstellungen**



Ports

Port Gerätekommunikation: Die Geräte verbinden sich mit diesem Port. (Standard: 30001)

> Änderungen an diesem Port dürfen nur durchgeführt werden, wenn gleichzeitig sicher gestellt wird, dass die Geräte die Verbindungsaufnahme ebenfalls auf dem neuen Port durchführen. Mehr Informationen zu Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).

Web-Serverport: Stellt die Verbindung zum Server her. Dieser Port muss im Anmeldefenster der IGEL UMS Konsole oder in der URL der UMS Web App (see page 786) eingegeben werden. (Standard: 8443)

> Wenn der Port geändert wird, muss der Dienst `IGEL RMGUIServer/igelRMserver` neu gestartet werden.

> ⚠ Falls keine Cluster-Adresse (see page 581) konfiguriert wurde, können die bereits registrierten IGEL OS 12-Geräte nach der Änderung des Web-Serverports nicht mehr verwaltet werden. Daher müssen Sie diese Geräte erneut registrieren.
> Wenn die Änderung des Web-Serverports erforderlich ist, empfiehlt es sich daher, den Port vor der Registrierung von IGEL OS 12-Geräten zu ändern.

HTTP port: Wenn **Verbindung nur über SSL zulassen** deaktiviert ist, wird dieser Port verwendet, um die UMS über eine unverschlüsselte Verbindung per HTTP zu erreichen. Damit dies möglich ist, muss dieser Port in der Verbindungs-URL angegeben werden, z.B. `http://<server>:9080/ums_filetransfer/`. (Standard: 9080)

Datenbank-Port (Embedded DB): Port für die Kommunikation mit der Embedded-DB. (Standard: 1528)
Für externe Datenbanken wird der Port unter **Datenquellen** definiert.

Verbindung nur über SSL zulassen

☑ Verbindung wird nur über SSL zugelassen. Dieser Parameter wird standardmäßig nur bei neuen UMS-Installationen ab UMS Version 12.02.100 aktiviert. (Standard)

Konfiguration Datenbankinstanz

Remote-Manager-ID (nur lesend): Eindeutiger Schlüssel der UMS Instanz. Wird automatisch ausgelesen.

Cipher (serverseitig)

Wichtig: Die Cipher-Konfiguration ist serverspezifisch und darum nicht in Datenbank-Backups enthalten.

Falls Sie UMS High Availabity (UMS) verwenden, müssen Sie die Cipher-Einstellungen für jeden Server separat vornehmen.

Cipher konfigurieren: Betätigen Sie die Schaltfläche, um den Dialog **Cipher Auswahl** zu öffnen. In diesem Dialog können Sie festlegen, welche Cipher vom UMS Server unterstützt werden.

Im Dialog **Cipher Auswahl** stehen Ihnen folgende Schaltflächen zur Verfügung:

- **Aktivieren**: Die in der linken Liste gewählte Cipher aktivieren.
- **Deaktivieren**: Die in der rechten Liste gewählte Cipher deaktivieren.
- **Defaults verwenden**: Die Cipherauswahl auf die Standardeinstellungen setzen.
  Liste von standardmäßigen Cipher Suites

  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
  TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
  TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- **Ok**: Die Änderungen speichern.
- **Abbrechen**: Alle Änderungen verwerfen.

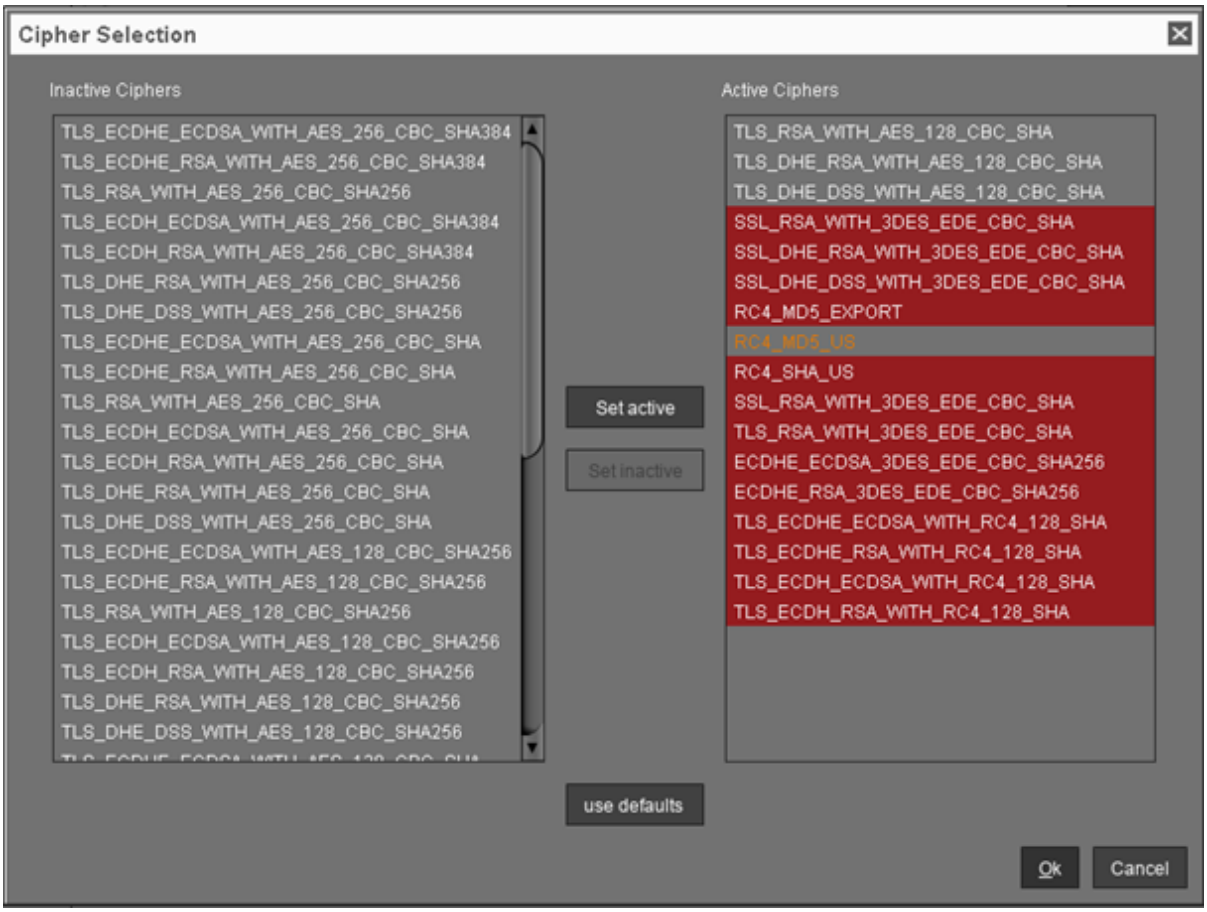
Bei neuen UMS Installationen werden nur die standardmäßigen Ciphers (see page 711) aktiviert. Bei Aktualisierung der bestehenden UMS Installationen bleiben die bereits konfigurierten Ciphers erhalten.

Wenn Ihr Server Ciphers aus vorangegangenen Installationen vorhält, kann es vorkommen, dass einige Ciphers nicht mehr als vertrauenswürdig eingestuft werden.

Die Sicherheitsstufen sind durch Farben repräsentiert:

- Normale Anzeigefarbe (schwarz oder weiß, abhängig vom eingestellten Erscheinungsbild): Die Cipher wird als vertrauenswürdig eingestuft und wird von Tomcat verwendet.
- Rote Farbe: Die Cipher wird nicht als vertrauenswürdig eingestuft und wird nicht von Tomcat verwendet. Diese Cipher kann nicht verwendet werden.
- Orange Farbe: Die Cipher wird von Tomcat verwendet, wird aber von IGEL, Tomcat oder einer anderen Institution nicht als vertrauenswürdig eingestuft. Es wird empfohlen, diese Cipher nicht zu verwenden.

Das folgende Beispiel enthält Ciphers mit allen 3 Sicherheitsstufen:



Cipher automatisch anpassen bei Update

☑ Bei jeder Aktualisierung werden alle neuen Chiffres automatisch aktiviert und alle schwachen Chiffren deaktiviert.

☐ Die Konfiguration der Chiffren wird nicht bei Aktualisierungen automatisch angepasst.

SSL-Zertifikate

Web-Zertifikate zurücksetzen (Nur für Disaster Recovery): Verwenden Sie diese Funktion nur, wenn Sie nicht über die UMS Konsole oder die UMS Web App auf den UMS Server zugreifen können. Diese Funktion deaktiviert die Zertifikatskette, die zuvor für die Kommunikation über den Web-Port verwendet wurde (d. h. über den für HTTPS verwendeten Port; Standard: 8443; weitere Informationen finden Sie unter IGEL UMS Kommunikationsports (see page 6)). Außerdem wird eine neue Zertifikatskette erstellt, die dann für HTTPS verwendet wird.

> ⓘ Wenn Sie Ihr eigenes Zertifikat oder Ihre eigene Zertifikatskette verwenden wollen, lesen Sie Using Your Own Certificates for Communication over the Web Port (Default: 8443) (see page 125).

UMS-ID-Sicherung im IGEL Administrator

Im IGEL UMS Administrator können Sie ein Backup der UMS-ID (vor UMS 12 als "UMS-Lizenz-ID" bezeichnet) erstellen. Informationen über die UMS-ID finden Sie auch unter UMS ID (see page 639).

> Standardpfad zum UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

Menüpfad: **UMS Administrator > UMS-ID-Sicherung**

> Die UMS-ID wird bei jeder Installation eines UMS Servers erzeugt. Wenn Sie also eine High-Availability- oder Distributed UMS-Umgebung (siehe IGEL UMS Installation (see page 246)) haben, hat jeder Server eine eigene UMS-ID, d. h. eine **lokale UMS-ID**. Für die Kommunikation aller UMS Server mit dem ILP und IGEL Cloud Services wird eine **Haupt-UMS-ID** verwendet.

Haupt-UMS-ID: Die ersten und letzten 10 Zeichen der Haupt-UMS-ID.

Fingerabdruck der Haupt-UMS-ID: Der SHA-256-Fingerabdruck der Haupt-UMS-ID.

Lokale UMS-ID: Die ersten und letzten 10 Zeichen der lokalen UMS-ID.

> In der High-Availability-Umgebung kann sich die lokale UMS-ID von der Haupt-UMS-ID unterscheiden. Sollte dies der Fall sein, starten Sie den Server zwecks Synchronisierung neu. Siehe auch Manuelle Synchronisierung der UMS-ID (see page 157).
> Dies gilt auch für die Distributed UMS-Installationen.

Fingerabdruck der lokalen UMS-ID: Der SHA-256-Fingerabdruck der lokalen UMS-ID.

Erstelle neue Haupt-UMS-ID: Wenn die Installation keine UMS-ID hat, dann wurde diese bei der Installation nicht angelegt und sie muss manuell erstellt werden.

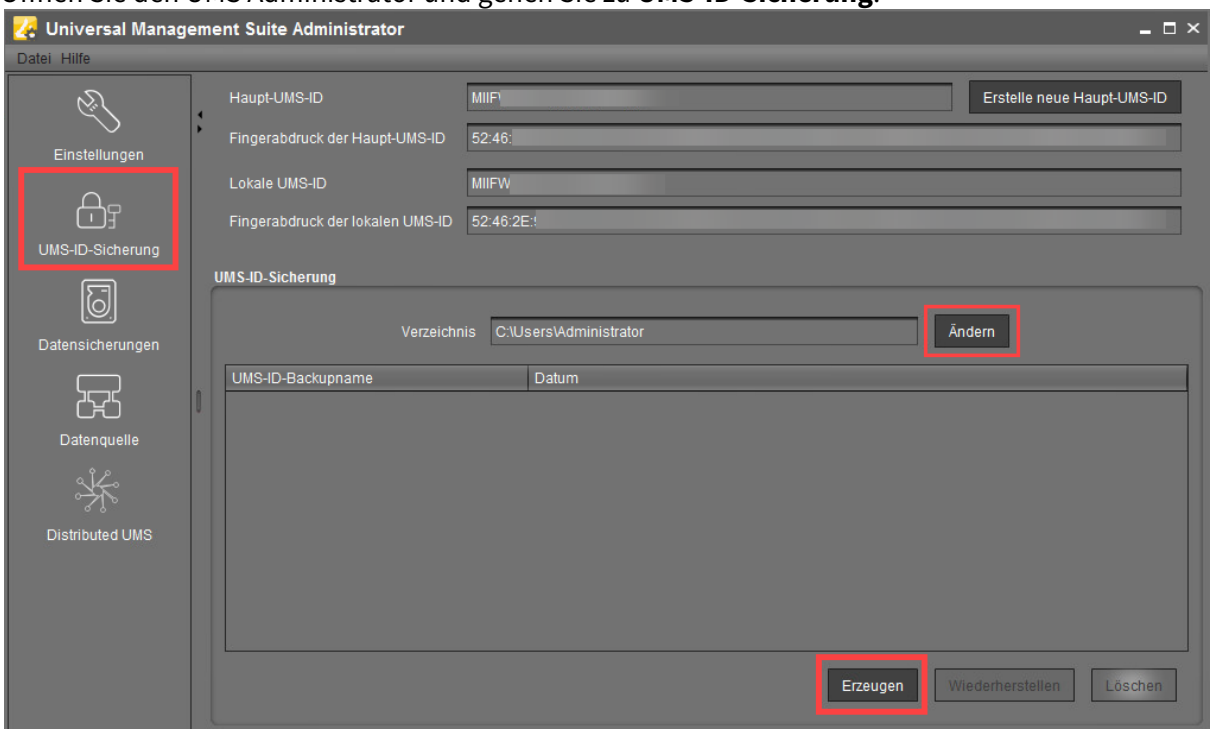
Verzeichnis: Pfad zum Speicherort des Backups.

UMS-ID-Backupname: Der Name des Backups, den Sie beim Erstellen vergeben haben.

Datum: Datum, wann das Backup erstellt wurde.

Ein Backup der UMS-ID erstellen

1. Öffnen Sie den UMS Administrator und gehen Sie zu **UMS-ID-Sicherung**.

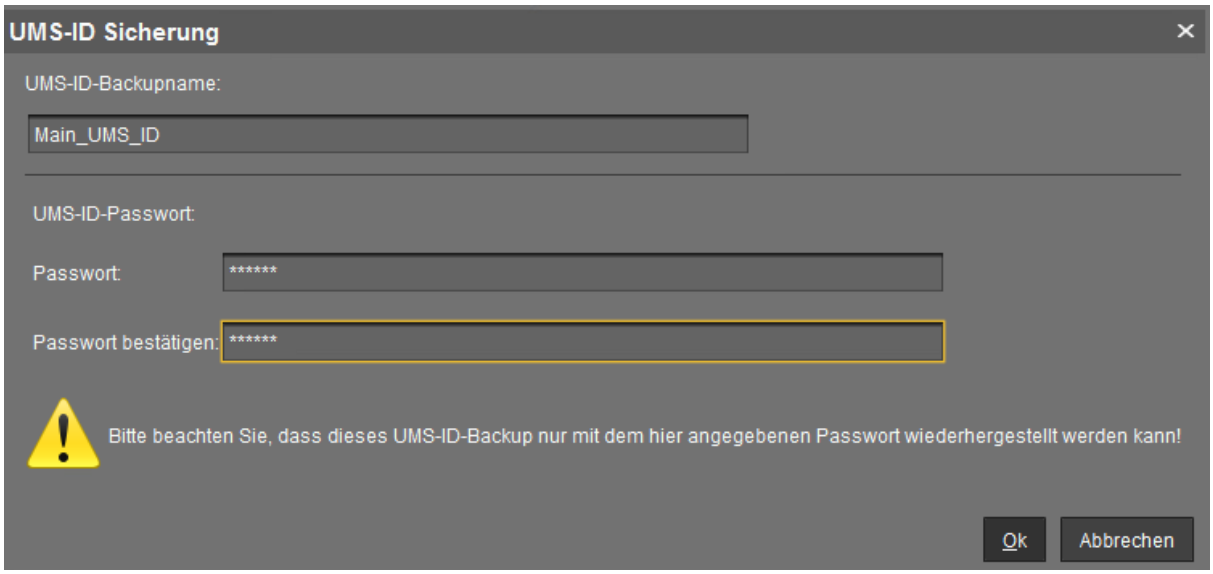


2. Klicken Sie **Ändern**, wenn Sie das Verzeichnis für die Speicherung des Backups ändern möchten.

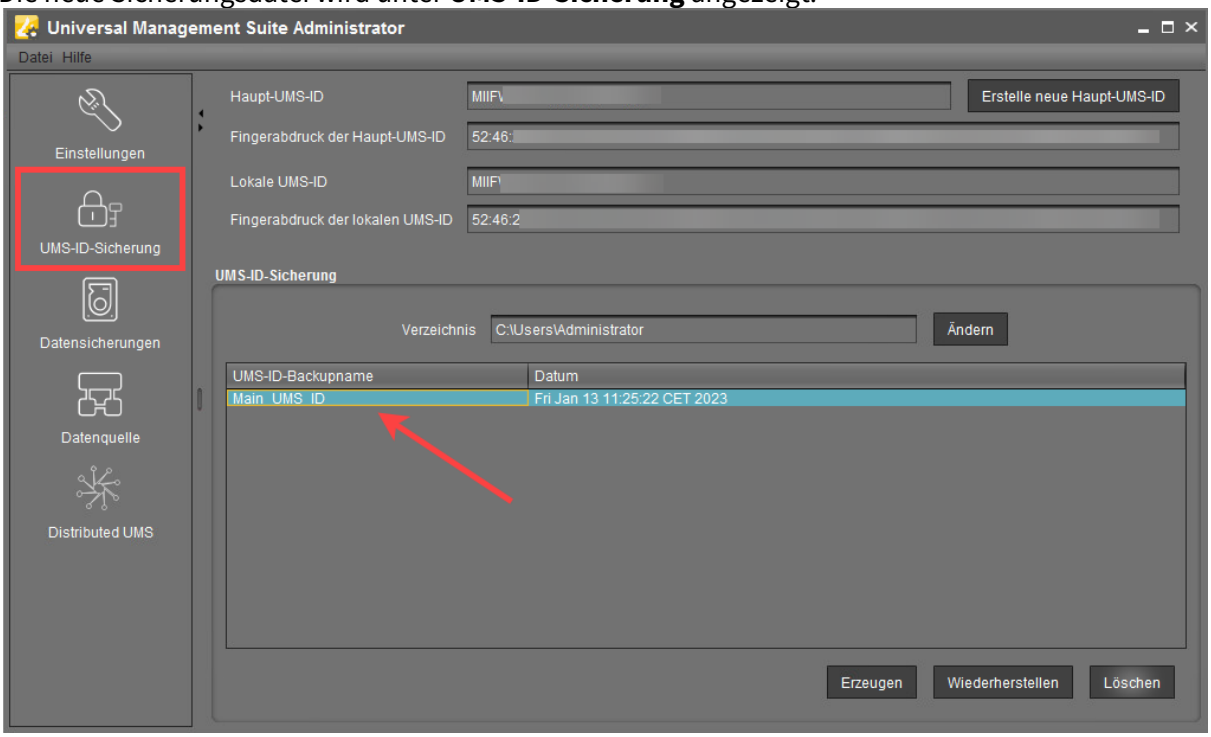
3. Klicken Sie **Erzeugen**.
   Der Dialog **UMS-ID Sicherung** öffnet sich.

   > Falls Sie eine High Availability- oder Distributed UMS-Umgebung verwenden, beachten Sie das Folgende:
   > Es ist immer die UMS-ID des lokalen Servers, die gesichert wird. Stellen Sie daher zunächst sicher, dass die **lokale UMS-ID** mit der **Haupt-UMS-ID** übereinstimmt. Wenn dies nicht der Fall ist, starten Sie den UMS Server neu, um die lokale UMS-ID mit der Haupt-UMS-ID zu synchronisieren. Dann fahren Sie mit der Erstellung des Backups fort. Siehe auch Manuelle Synchronisierung der UMS-ID (see page 157).

4. Geben Sie einen **Namen** für das UMS-ID-Backup und ein **Passwort** ein. Merken Sie sich das Passwort, sonst können Sie das Backup nicht wiederherstellen.

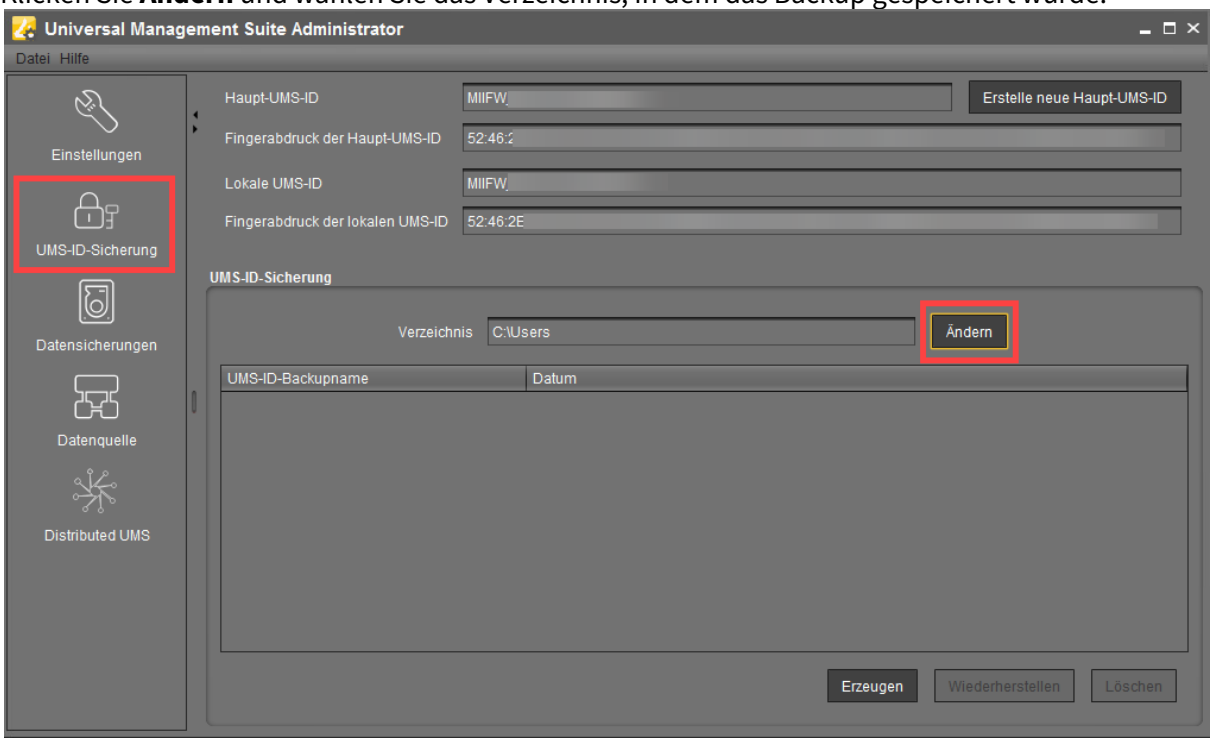


5. Klicken Sie **OK**.
   Die neue Sicherungsdatei wird unter **UMS-ID-Sicherung** angezeigt.



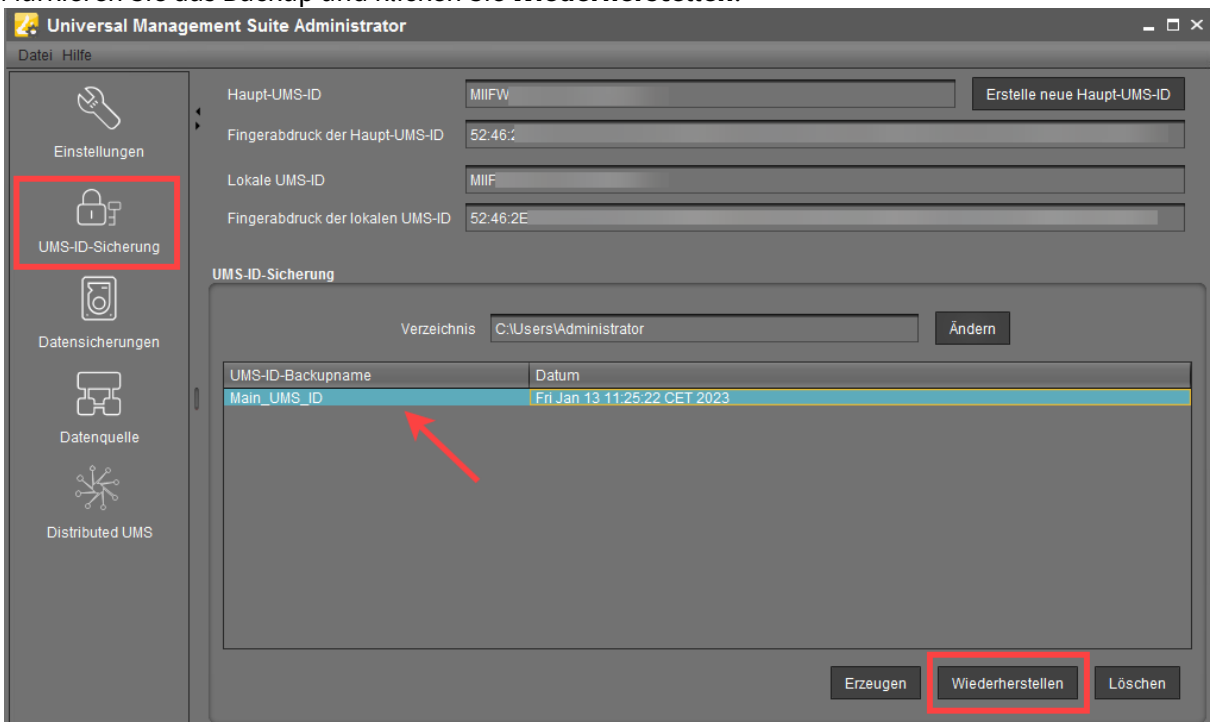
Ein Backup der UMS-ID wiederherstellen

1. Öffnen Sie den UMS Administrator und gehen Sie zu **UMS-ID-Sicherung**.
2. Klicken Sie **Ändern** und wählen Sie das Verzeichnis, in dem das Backup gespeichert wurde.



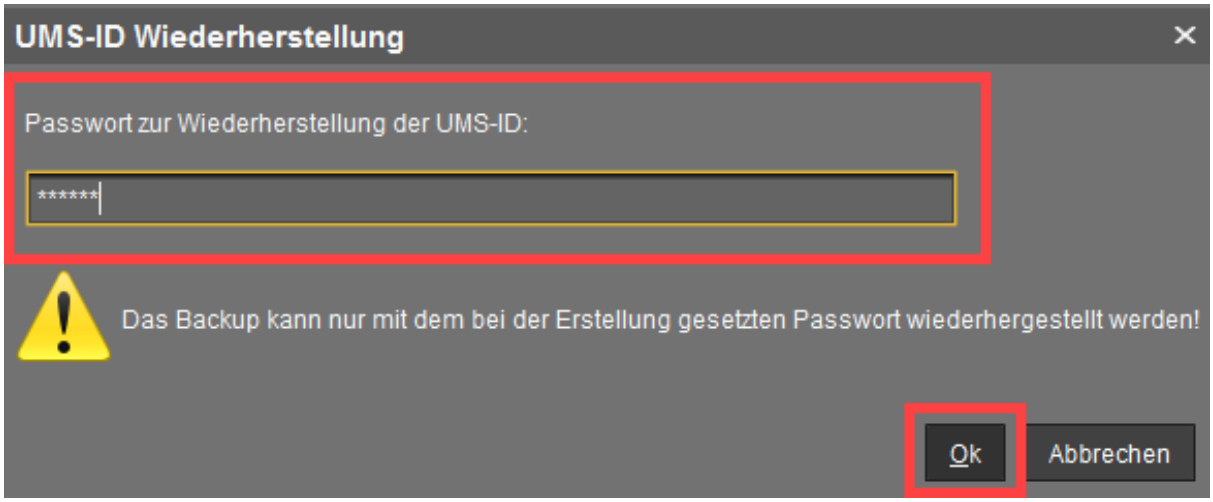
Das Backup erscheint in der Liste der verfügbaren UMS-ID-Backups.

3. Markieren Sie das Backup und klicken Sie **Wiederherstellen**.

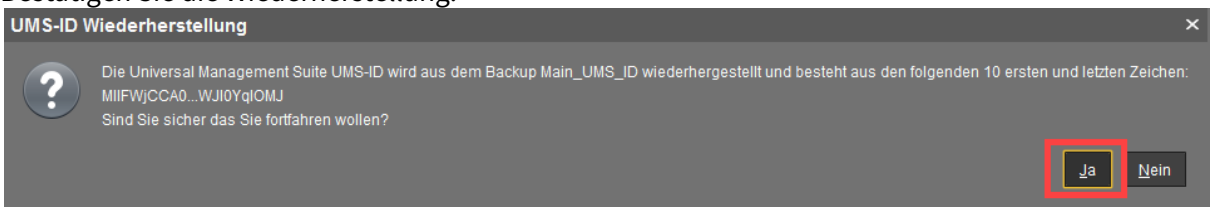


Der Dialog **UMS-ID Wiederherstellung** öffnet sich.

4. Geben Sie das **Passwort** ein und klicken Sie **OK**.



5. Bestätigen Sie die Wiederherstellung.



Datensicherungen

Menüpfad: **UMS Administrator > Datensicherungen**

> Standardpfad zum UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

Die interne Embedded-DB des UMS Servers kann direkt über den UMS Administrator gesichert werden. Es lassen sich auch zuvor erstellte Backups wieder einspielen.

- Ein Backup der IGEL UMS erstellen (see page 720)
- Backup wiederherstellen (see page 725)
- Backup löschen (see page 727)
- Zeitgesteuertes Backup (see page 728)

> Für externe Datenbanksysteme verwenden Sie bitte die vom DBMS-Hersteller vorgesehene Vorgehensweise zu Backup und Recovery. Für weitere Informationen siehe Ein Backup der IGEL UMS erstellen (see page 720).

Ein Backup der IGEL UMS erstellen

Der folgende Artikel erklärt, wie Sie ein Backup Ihrer IGEL Universal Management Suite (UMS) Installation erstellen können.

Menüpfad: **UMS Administrator > Datensicherungen**

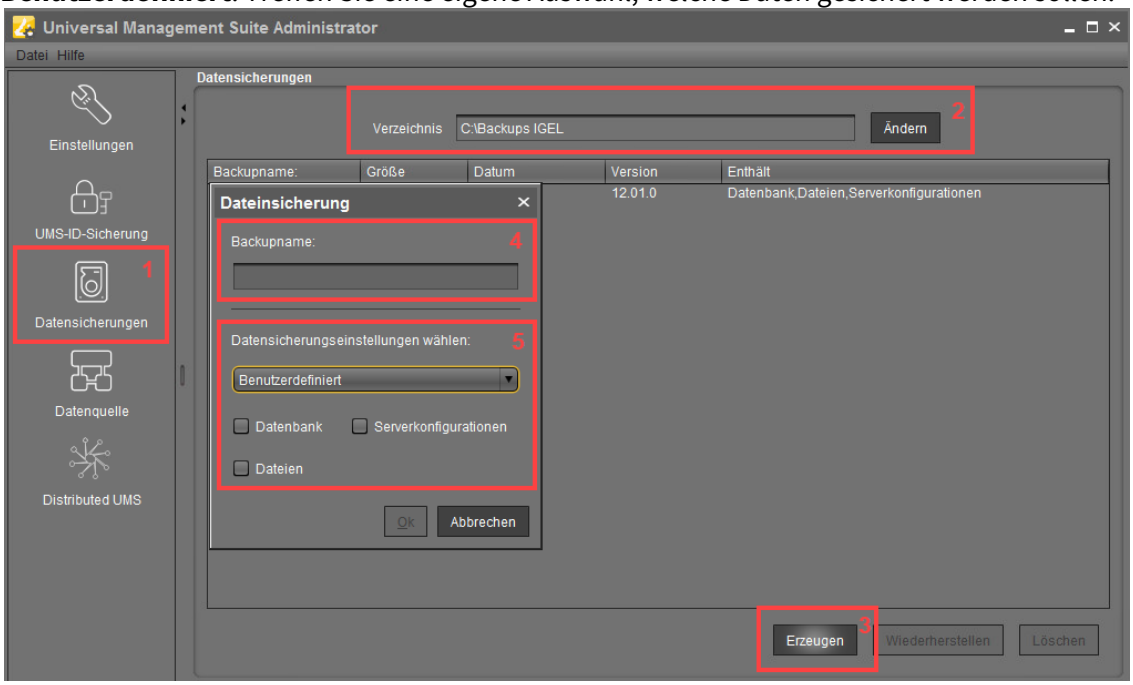
> Standardpfad zum UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

Embedded-Datenbank

So erstellen Sie ein Backup der UMS Installation mit der Embedded-Datenbank:

1. Öffnen Sie den UMS Administrator und wählen Sie **Datensicherungen**.
2. Klicken Sie **Ändern**, um den Speicherort für Ihre Backups zu ändern.
3. Klicken Sie **Erzeugen**.
4. Geben Sie unter **Backupname** einen Namen für dieses Backup ein.
5. Wählen Sie die **Datensicherungseinstellungen**:
   Wählbar sind:
   - **Alle auswählen** (Standard): Datenbank, Serverkonfigurationen (see page 721) und Dateien (normalerweise werden Sie diese Option verwenden, um sicherzustellen, dass keine Komponenten im Backup fehlen)
   - **Embedded Datenbank**: Datenbank
   - **Alle Dateien**: Dateien (z. B. Bilder, Sitzungszertifikate)
     Beachten Sie: Dateien, die nicht in der UMS registriert wurden, sondern nur in den System-Webressourcen abgelegt sind (z. B. manuell im Ordner `ums_filetransfer` abgelegt wurden), werden vom UMS Administrator NICHT gesichert.

- **Benutzerdefiniert**: Treffen Sie eine eigene Auswahl, welche Daten gesichert werden sollen.



- Ab UMS Version 5.09 werden alle Zertifikate in das Datenbankbackup aufgenommen.
- Ab UMS Version 6.08 werden alle Gerätelizenzen in das Datenbankbackup aufgenommen. Backups von Lizenzen, die mit den früheren UMS Versionen erstellt wurden, werden unterstützt: Wenn Sie das Backup wiederherstellen, werden die im Backup gespeicherten Lizenzdateien in der Datenbank gespeichert; siehe Backup wiederherstellen (see page 725).

Universal Firmware Updates

Die Firmwaredateien sind nicht Teil des UMS Embedded-DB Backups. Sie sind nicht im **Dateien**-Backup enthalten und müssen daher manuell aus `[IGEL Installationsverzeichnis]/rmguiserver/webapps/ums_filetransfer` kopiert werden.

Das Backup der **Serverkonfigurationen** enthält die meisten Konfigurationen des Bereichs Einstellungen (see page 709) im UMS Administrator. Ausnahmen: **Web-Serverport**, **JWS-Serverport** und **Ciphers** – sie sind hostspezifisch, d.h. sie werden auf jedem Server separat gespeichert und können nicht Teil eines Backups sein. Daher sollten Sie die Werte dieser Einstellungen notieren, wenn sie vom Standard abweichen, und im Falle eines Recovery-/Migrationsverfahrens müssen sie auf jedem Server manuell angepasst werden.

6. Bestätigen Sie die Auswahl mit **OK**.
   Die Daten werden in dem von Ihnen gewählten Verzeichnis gespeichert.

   Denken Sie daran, auch die UMS-ID zu sichern, siehe UMS-ID-Sicherung im IGEL Administrator (see page 713).

Externe Datenbank

Sämtliche Backup-Optionen sind nur verfügbar, wenn Sie die eingebettete Datenbank für Ihre UMS Serverinstallation verwenden.

Wenn Sie eine externe Datenbank (see page 308) verwenden, gehen Sie wie folgt vor, um ein vollständiges Backup Ihres Systems zu erstellen:

1. Für die Datenbank selbst verwenden Sie die vom DBMS-Hersteller vorgesehene Vorgehensweise zu Backup und Recovery.

   Zertifikate

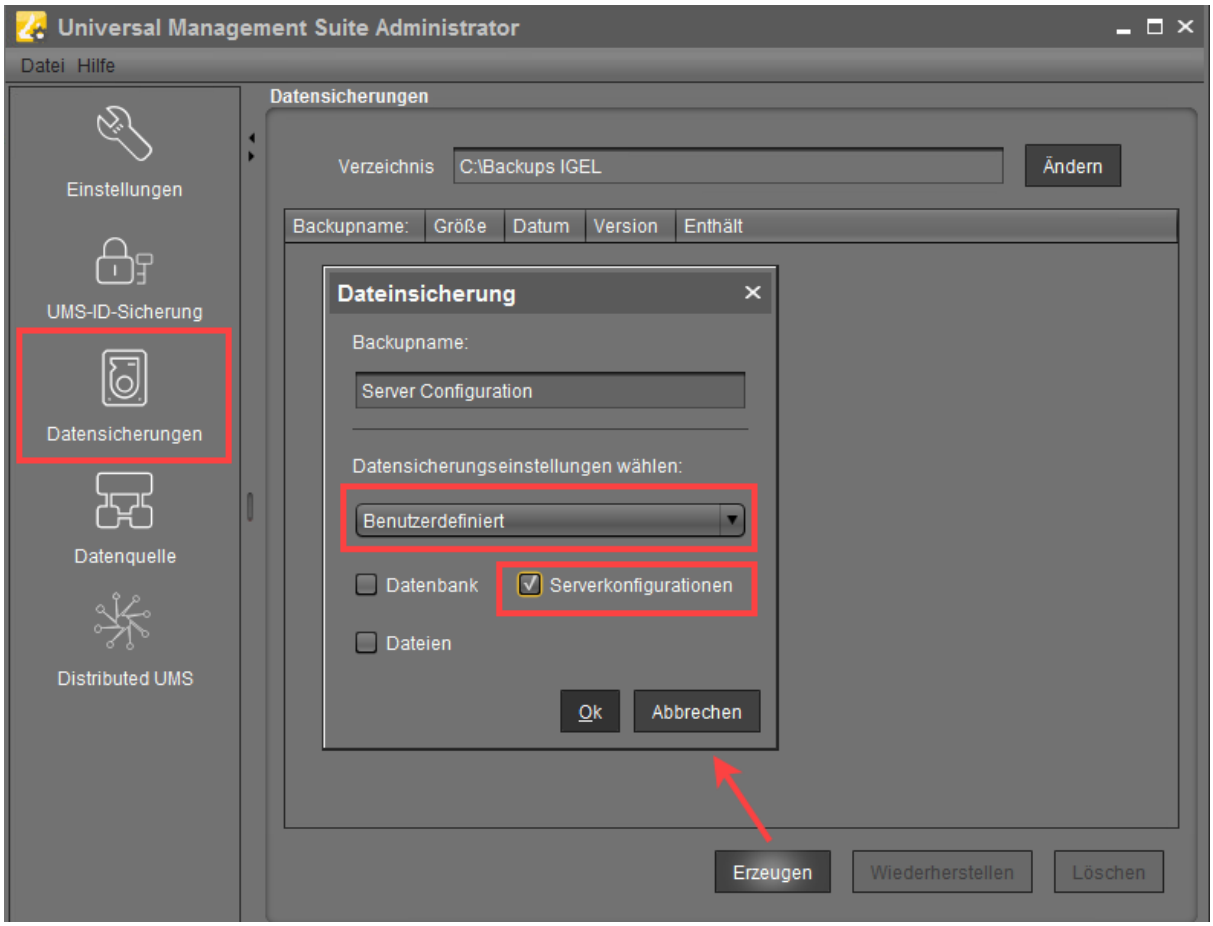
   Ab UMS Version 5.09 werden alle Zertifikate in das Datenbankbackup aufgenommen.
   Wenn Sie die Zertifikate manuell sichern müssen, finden Sie sie hier:

   - `[IGEL Installationsverzeichnis]/rmtcserver/*`
     Es enthält die Datei `tc.keystore`, die für die Kommunikation mit den Endgeräten notwendig ist. Das Zertifikat dieses Keystores kann auch über die UMS Konsole unter **UMS Administration > Globale Konfiguration > Zertifikatsverwaltung > Gerätekommunikation > Schlüsselpaar exportieren** exportiert werden  .
   - `[IGEL Installationsverzeichnis]/rmclient/cacerts`
   - `[IGEL Installationsverzeichnis]/rmguiserver/https_cert_chain.keystore`

   Lizenzen

   Ab UMS Version 6.08 werden alle Gerätelizenzen in das Datenbankbackup aufgenommen. Bisher wurden sie in `[IGEL Installationsverzeichnis]/rmguiserver/webapps/e08ce61-d6df-4d2b-b44a-14c1ec722c44` gespeichert und mussten separat gesichert, d.h. manuell auf ein sicheres Speichermedium kopiert werden.

2. Sichern Sie die Serverkonfigurationen über **UMS Administrator > Datensicherungen > Erzeugen > Benutzerdefiniert > Server Konfigurationen**. Notieren Sie separat hostspezifische Konfigurationen, die vom Standard abweichen, siehe oben Serverkonfigurationen (see page 721):



3. Dateien und Firmwareupdates müssen separat gesichert, d.h. manuell auf ein sicheres Speichermedium kopiert werden. Hier finden Sie sie: `[IGEL Installationsverzeichnis]/rmguiserver/webapps/ums_filetransfer`

4. Sichern Sie auch die UMS-ID, siehe UMS-ID-Sicherung im IGEL Administrator (see page 713).

   > Falls Sie eine High Availability- oder Distributed UMS-Umgebung verwenden, beachten Sie das Folgende:
   > Es ist immer die UMS-ID des lokalen Servers, die gesichert wird. Stellen Sie daher zunächst sicher, dass die **lokale UMS-ID** mit der **Haupt-UMS-ID** übereinstimmt. Wenn dies nicht der Fall ist, starten Sie den UMS Server neu, um die lokale UMS-ID mit der Haupt-UMS-ID zu synchronisieren. Dann fahren Sie mit der Erstellung des Backups fort. Siehe auch Manuelle Synchronisierung der UMS-ID (see page 157).

5. Nur für HA-Installationen (see page 909): Speichern Sie das aktuelle IGEL Netzwerktoken (ermöglicht die Integration neuer Server in dasselbe HA-Netzwerk). Dies ist in der Regel ein während der Installation erstelltes Token, siehe Ersten Server in einem HA-Netzwerk installieren (see page

917). Wurde inzwischen ein neues IGEL Netzwerktoken generiert, z. B. wenn Änderungen an Zertifikaten vorgenommen wurden (siehe "High Availability" unter Gerätekommunikation (see page 573)), ist dies das zu sichernde Token.

Backup wiederherstellen

Menüpfad: **UMS Administrator > Datensicherungen**

> Standardpfad zum UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

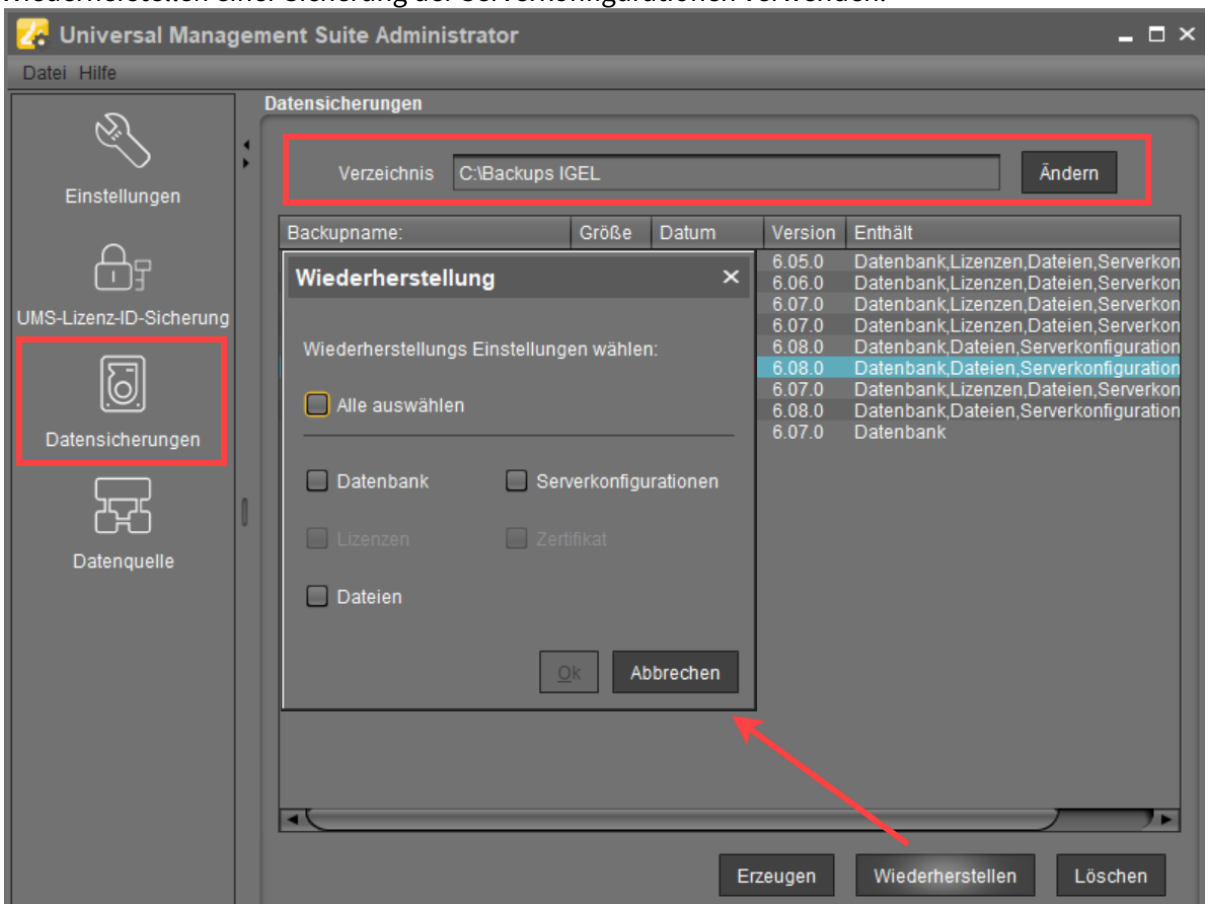
> Beim Wiederherstellen eines Backups wird Ihr aktueller Datenbankstatus überschrieben. Es wird dringend empfohlen, ein Backup der aktuellen Daten zu erstellen, bevor ein anderes Backup wiederhergestellt wird, siehe Ein Backup der IGEL UMS erstellen (see page 720).

> Wenn Sie ein Datenbank-Backup einer eingebetteten Datenbank aus einer UMS Version vor 6.05 wiederherstellen, sind die Anmeldedaten des Superusers mit den Anmeldedaten des Datenbankbenutzer identisch. Es wird empfohlen, das Passwort des Superusers zurückzusetzen.
> Bei Datenbank-Backups von UMS Versionen ab 6.05 sind die Anmeldedaten des Superusers bereits im Datenbank-Backup gespeichert und werden von dort übernommen.

So stellen Sie ein gespeichertes Backup wieder her:

1. Prüfen Sie unter **UMS Administrator > Datensicherungen**, ob das **Verzeichnis** dasjenige ist, das Ihr Backup enthält; falls nicht, klicken Sie **Ändern**, um zum richtigen Verzeichnis zu wechseln.
2. Wählen Sie das gewünschte Backup aus der Backupliste aus.
3. Klicken Sie auf **Wiederherstellen**.
4. Wählen Sie die Komponenten aus, die wiederhergestellt werden sollen.
   In UMS Installationen mit externer Datenbank können Sie den UMS Administrator nur zum

Wiederherstellen einer Sicherung der Serverkonfigurationen verwenden.



Die Optionen **Zertifikat** und **Lizenzen** sind ausgegraut, da ab UMS Version 5.09 bzw. 6.08 Zertifikate und Lizenzen in das Datenbankbackup aufgenommen werden.

Nach erfolgter Wiederherstellung werden die Anmeldedaten zur Datenbank angezeigt.

Tipp
Um Probleme mit der Wiederherstellung von Backups und allgemein mit der Leistung der UMS zu vermeiden, wird dringend empfohlen, administrative Aufgaben zur automatischen Löschung von Protokollen – Logging-Informationen, Ergebnissen von Aufgaben, Ergebnissen von administrativen Aufgaben, Prozessereignissen, Verlauf der Assetinformationen – zu verwenden; siehe Administrative Aufgaben - Zeitlich geplante Aktionen für die IGEL UMS konfigurieren (see page 597). Siehe auch Leistungsoptimierungen (see page 294).

Backup löschen

Menüpfad: **UMS Administrator > Datensicherungen**

> Standardpfad zum UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

So löschen Sie ein gespeichertes Backup:

1. Wählen Sie das gewünschte Backup aus der Backupliste aus.
2. Klicken Sie **Löschen**, um nicht mehr benötigte Backups zu entfernen.

   > Es wird sowohl der Eintrag im UMS Administrator wie auch die Backupdatei auf der Festplatte gelöscht!

Zeitgesteuertes Backup

Sie können ein geplantes Backup unter **UMS Administration > Administrative Aufgaben** definieren, siehe Datensicherung erstellen (see page 599).

Datenquelle

Menüpfad: **UMS Administrator > Datenquelle**

Die Anbindung an ein Datenbanksystem erfolgt über Datenquellen, die Sie im UMS Administrator verwalten.

> Standardpfad zum UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

Haben Sie die Standardinstallation gewählt, ist die Embedded-DB bereits als Datenquelle eingerichtet und aktiviert.

Siehe auch Anbindung externer Datenbanksysteme (see page 308).

Wie kann ich eine Datenquelle im IGEL UMS Administrator einrichten?

Menüpfad: **UMS Administrator > Datenquelle**

Der folgende Artikel beschreibt, wie Sie eine Datenquelle für die IGEL Universal Management Suite (UMS) konfigurieren können.

Die IGEL UMS unterstützt die folgenden Datenquellentypen:

- Embedded DB (installiert über die IGEL UMS)
- Microsoft SQL Server
- Oracle
- PostgreSQL
- Apache Derby

> Angaben zu den unterstützten Datenbanksystemen finden Sie in den Release Notes (see page 965) im Bereich "Supported Environment". Die Installations- und Betriebsvoraussetzungen für die Datenbank finden Sie in der Dokumentation des jeweiligen DBMS.

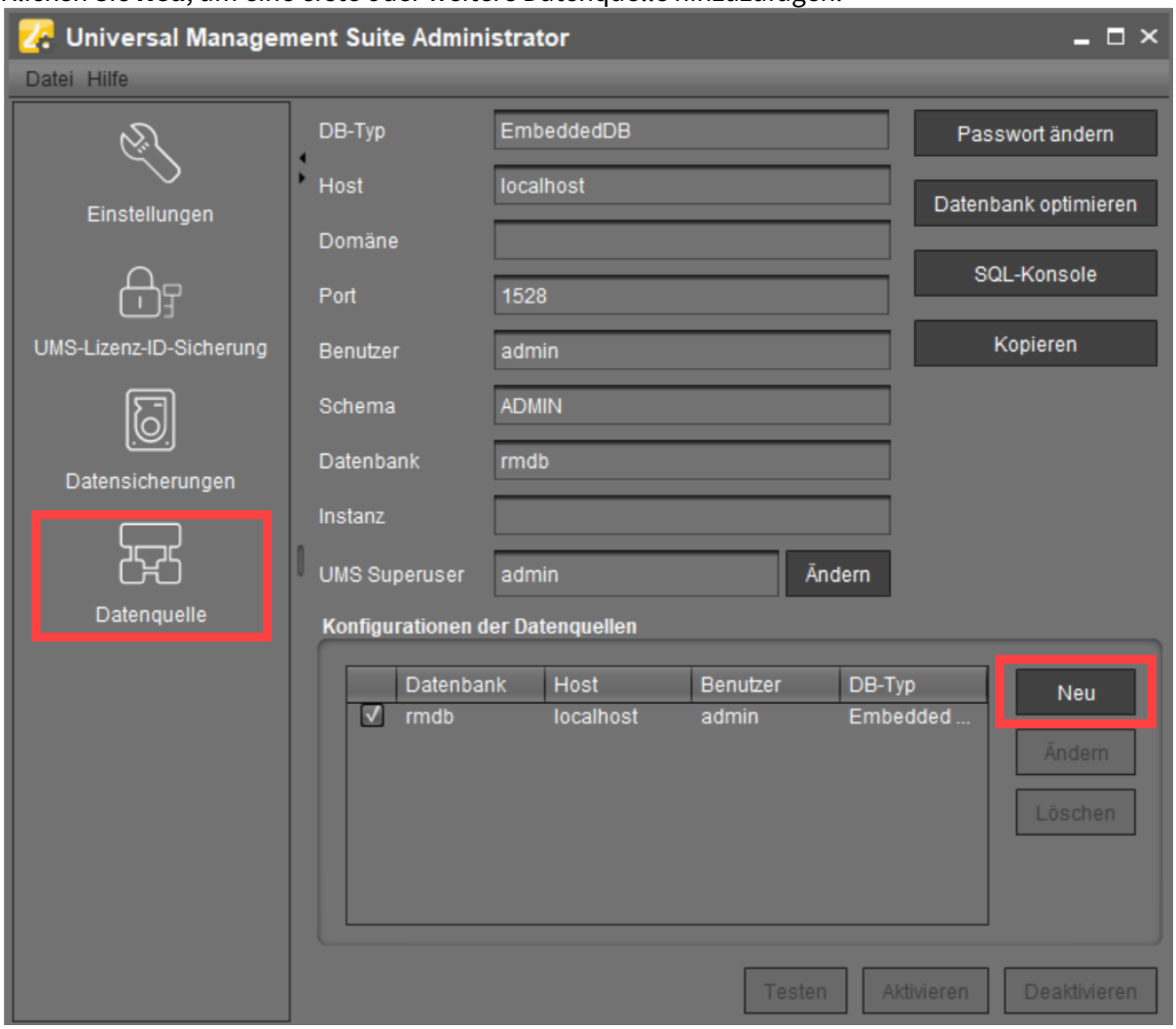
Informationen zu den externen Datenbanksystemen finden Sie auch unter Anbindung externer Datenbanksysteme (see page 308).

> Standardpfad zum UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

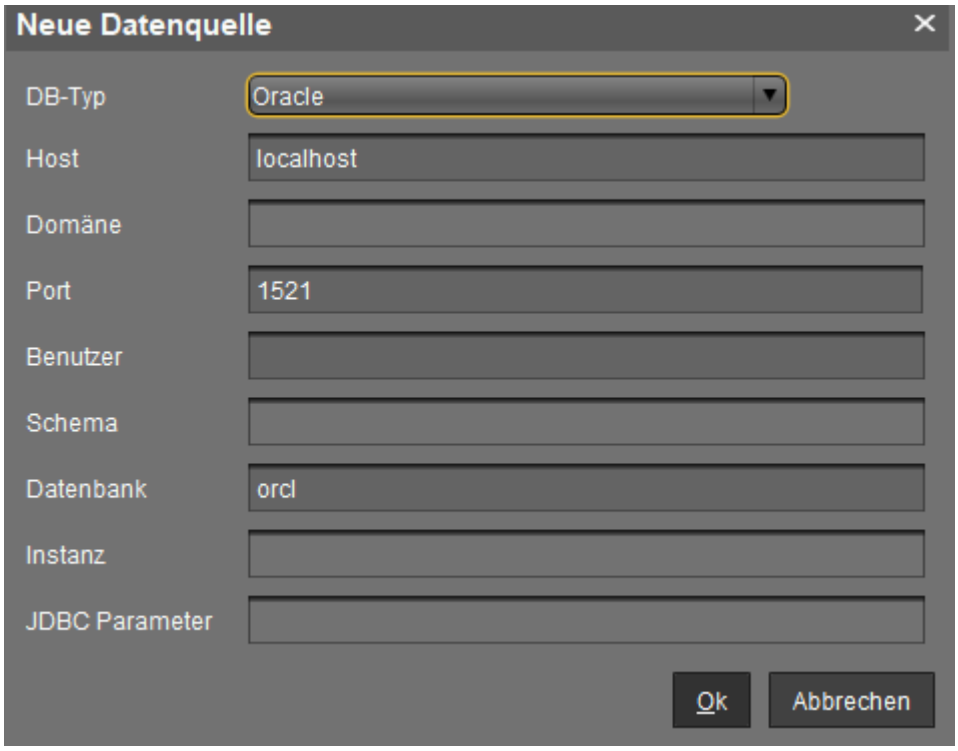
Datenbankverbindung im IGEL UMS Administrator hinzufügen

So legen Sie die Datenquelle an:

1. Klicken Sie **Neu**, um eine erste oder weitere Datenquelle hinzuzufügen.



Ein Dialogfenster **Neue Datenquelle** öffnet sich.



2. Wählen Sie den **DB-Typ** und geben Sie den **Host** und **Port** für den Verbindungsaufbau sowie den am DBMS eingerichteten **Benutzer** ein. Für SQL Server Cluster und Oracle RAC ist die **Instanz** anzugeben.

   > Solange eine Datenquelle nicht aktiviert wurde, lassen sich diese Einstellungen über **Ändern** noch anpassen. Die aktive Datenquelle ist vor Konfigurationsänderungen geschützt. Über **Passwort ändern** können Sie ein neues Passwort für den Datenbankbenutzer setzen. Das ist auch bei aktivierter Datenquelle möglich.

   > Wenn Sie MS SQL Server AlwaysOn-Verfügbarkeitsgruppen (Availability Groups) verwenden, setzen Sie **DB-Typ** auf **SQL Server** und geben Sie unter **Host** einen Domänennamen des Listeners für AlwaysOn-Verfügbarkeitsgruppen an.

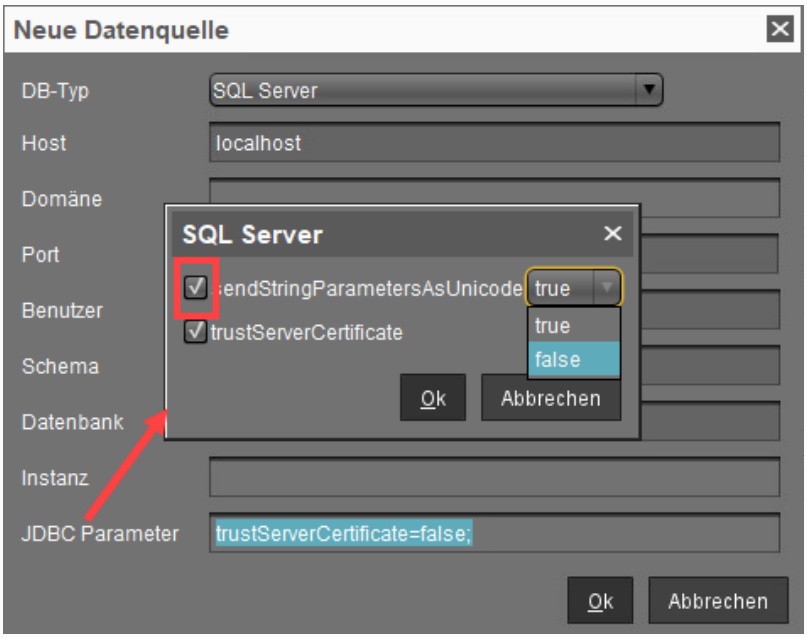
   > Mittels **JDBC Parameter** können Sie zusätzliche Parameter definieren, die der JDBC-URL hinzugefügt werden. Derzeit werden die folgenden Parameter unterstützt:
   >
   > - Microsoft SQL Server: `sendStringParametersAsUnicode` (Standardwert: `true`)
   >
   >   Dieser Parameter kann angepasst werden, um die Abfrageleistung in einigen Fällen zu verbessern. Siehe den Microsoft-Artikel setSendStringParametersAsUnicode Method (SQLServerDataSource)[34].

34 https://docs.microsoft.com/en-us/sql/connect/jdbc/reference/setsendstringparametersasunicode-method-sqlserverdatasource?view=sql-server-ver16

- Microsoft SQL Server: `trustServerCertificate` (Standardwert: `false`)
  Dieser Parameter kann geändert werden, um die Zertifikatsprüfung von Verbindungen von der UMS zur Datenbank zu bestimmen. Siehe den Microsoft Artikel Connecting with encryption - JDBC Driver for SQL Server[35].
  Bitte folgen Sie den Anweisungen im Microsoft Artikel, wenn Sie die Eigenschaft auf '`false`' setzen möchten.

  Zwecks Abwärtskompatibilität wird die Eigenschaft auf '`true`' gesetzt, wenn im Feld **JDBC Parameter** des UMS Administrators kein Wert angegeben wird. Neue Datenquellendefinitionen werden standardmäßig mit dem Wert '`false`' für die Eigenschaft erstellt.

▶ Um den Parameter zu aktivieren und den Wert zu ändern, klicken Sie auf das Textfeld **JDBC Parameter**.



3. Klicken Sie **Test**, um die Verbindung zur Datenbank zu testen.
   Das ist auch bei inaktiven Datenquellen möglich.

4. **Aktivieren** Sie bei Bedarf die Datenquelle. Siehe Datenquelle aktivieren (see page 734).

35 https://learn.microsoft.com/en-us/sql/connect/jdbc/connecting-with-ssl-encryption?view=sql-server-ver16

Datenquelle aktivieren

Menüpfad: **UMS Administrator > Datenquelle**

> Standardpfad zum UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

Sie können mehrere Datenquellen anlegen. Es kann aber nur eine aktiv vom Server verwendet werden.

So aktivieren Sie diese Datenquelle:

1. Wählen Sie aus der Liste der eingerichteten Datenquellen eine aus.
2. Klicken Sie **Aktivieren**.
3. Geben Sie das Passwort für die ausgewählte Datenquelle ein.
   Während der Aktivierung der Datenquelle prüft die Anwendung, ob ein gültiges Datenbankschema gefunden werden kann. Wenn kein Schema gefunden wird, erfolgt die Erstellung eines neuen Schemas. Ein veraltetes Schema wird aktualisiert, und wenn das Schema unbekannte Daten enthält, werden diese überschrieben.
4. Bestätigen Sie jede dieser Aktionen.

   > Das Überschreiben vorhandener Daten bedeutet, dass das gesamte Datenbankschema gelöscht wird, nicht nur die von IGEL UMS verwendeten veralteten Tabellen.

Datenquelle kopieren

Menüpfad: **UMS Administrator > Datenquelle**

> Standardpfad zum UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

So steigen Sie von der Standardinstallation mit Embedded-DB auf ein externes Datenbanksystem um, z. B. auf ein Oracle RAC-Cluster:

1. Bereiten Sie die neue Datenbank entsprechend der UMS-Installationsanweisung vor.
2. Legen Sie eine passende neue Datenquelle für dieses DBMS an.
3. Wählen Sie die noch aktive Datenquelle der Embedded-DB aus.
4. Klicken Sie **Kopieren**.
5. Wählen Sie die Zieldatenquelle aus.
6. Starten Sie den Prozess nach Eingabe der Anmeldedaten des Ziels.
7. Aktivieren Sie die neue Datenquelle.

Aktive Embedded-DB optimieren

Menüpfad: **UMS Administrator > Datenquelle**

> Standardpfad zum UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

▶ Klicken Sie **Datenbank optimieren**, um eine aktive Embedded-Datenbank zu optimieren.
Der Datenbankinhalt wird neu strukturiert.
Der Datenbankindex wird neu erstellt, um die Operationen auf der Datenbank zu beschleunigen.
Ein Nachrichtenfenster informiert über den erfolgreichen Abschluss dieses Vorgangs.

UMS Superuser ändern

Menüpfad: **UMS Administrator > Datenquelle**

Der UMS Superuser wird während des Installationsvorgangs erstellt. Dieser Benutzer wird für die erste Anmeldung an der UMS Konsole benötigt sowie für weitere Konfigurationsaufgaben, insbesondere die Einrichtung weiterer Administratorkonten mit eingeschränkten Rechten. Der UMS Superuser hat volle Zugriffsrechte.

Sie können den UMS Superuser ändern, wobei der Benutzer für die Datenbankverbindung unverändert bleibt.

> ⚠ In einer HA-Umgebung kann das Ändern des UMS Superusers im laufenden Betrieb zu Problemen führen, wenn die Server Dateien austauschen. Diese Probleme sind jedoch temporär.

▶ Klicken Sie **Ändern** neben dem Feld **UMS Superuser**, um **Benutzername** und **Passwort** für den UMS Superuser zu ändern.

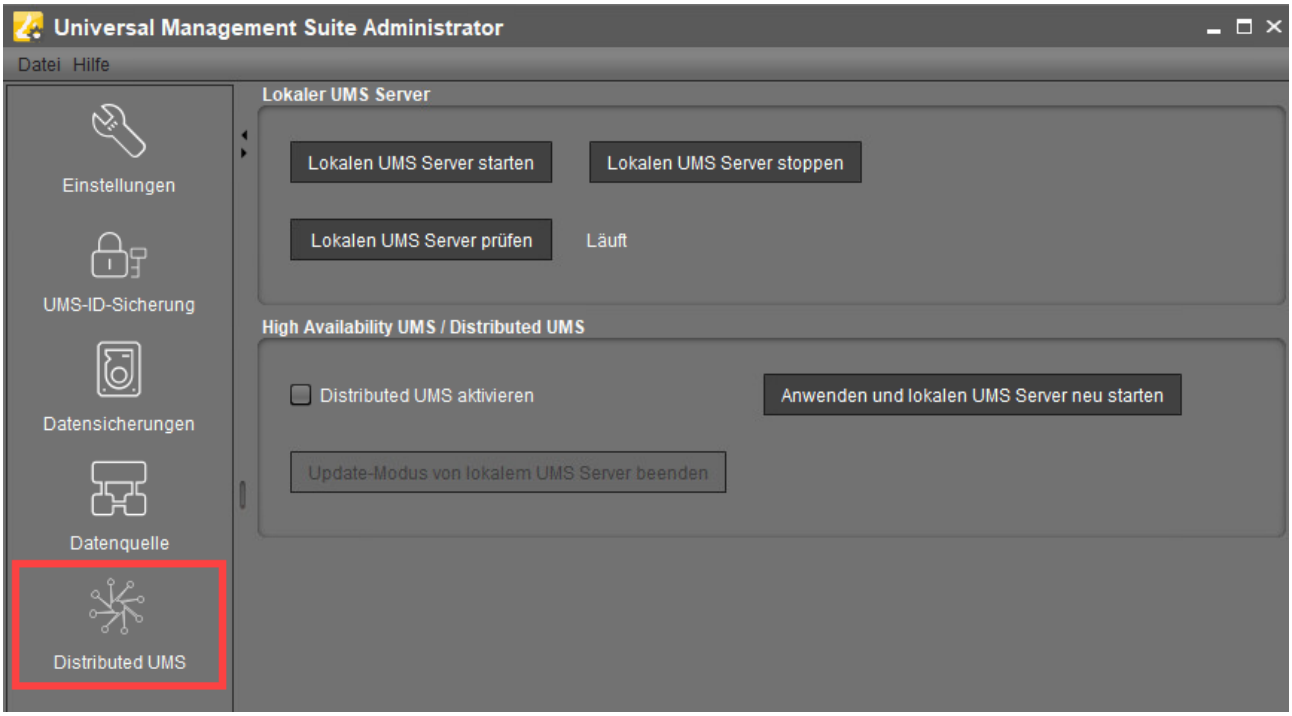
Distributed UMS - Lokale UMS-Aktionen im IGEL UMS Administrator ausführen

In diesem Bereich des IGEL Universal Management Suite (UMS) Administrators können Sie den lokalen UMS Server starten oder stoppen, den Update-Modus beenden und die Distributed UMS aktivieren.

Allgemeine Informationen zum UMS Administrator finden Sie unter Der IGEL UMS Administrator (see page 707).

> Standardpfad zum UMS Administrator:
> Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
> Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
> Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

Menüpfad: **UMS Administrator > Distributed UMS**



Lokalen UMS Server starten

Startet den UMS Server-Dienst auf diesem Rechner. Es kann einige Zeit dauern, bis der UMS Server-Dienst vollständig gestartet ist.

Für weitere Optionen zum Starten / Stoppen von Diensten siehe IGEL UMS HA-Dienste und -Prozesse (see page 949).

Lokalen UMS Server stoppen

Stoppt den UMS Server-Dienst auf diesem Rechner. Es kann einige Zeit dauern, bis der UMS Server-Dienst vollständig gestoppt ist.

Lokalen UMS Server prüfen

Prüft den Status des UMS Server-Dienstes auf diesem Rechner.

Mögliche Zustände:

- **Läuft**: Der lokale UMS Server ist aktiv und läuft.
- **Unterbrochen**: Der lokale UMS Server ist gestoppt.
- **Unbekannt**: Der Status des UMS Server-Dienstes ist unbekannt, z. B. wenn der `IGEL RMGUIServer` -Dienst gerade manuell über die Windows Dienste gestoppt/gestartet/pausiert wurde.

Distributed UMS aktivieren

Die Standalone UMS Server funktionieren so, als ob sie als High Availability-Umgebung installiert wären, wenn sie mit derselben externen Datenbank verbunden sind. Die Nachrichten zwischen den UMS Servern werden über Datenbankeinträge übertragen. Ausführliche Informationen über die Distributed UMS finden Sie unter IGEL UMS Installation (see page 246).

Informationen zur Installation der Distributed UMS oder zur Erweiterung einer bestehenden UMS Standardinstallation auf die Distributed UMS finden Sie unter Distributed IGEL UMS installieren (see page 275).

⚠ Wenn Sie die Distributed UMS-Funktion aktiviert haben und über mehrere UMS Server verfügen, seien Sie vorsichtig, falls Sie die Funktion deaktivieren möchten. Wenn die Distributed UMS-Funktion deaktiviert wird, aber mehrere UMS Server dieselbe Datenbank verwenden, wird keine Synchronisierung zwischen den UMS Servern durchgeführt.

ⓘ Wenn Sie eine UMS High Availability-Installation haben, wird dieses Kontrollkästchen ausgegraut und kann nicht aktiviert werden.

Anwenden und lokalen UMS Server neu starten

Die unter **Distributed UMS aktivieren** vorgenommenen Änderungen werden übernommen, und der UMS Server-Dienst auf diesem Rechner wird neu gestartet.

Update-Modus von lokalem UMS Server beenden

Verwenden Sie diese Funktion, wenn Sie Ihre Distributed UMS- oder UMS High Availability-Installation aktualisiert haben, der Update-Modus aber nicht automatisch beendet wurde, als der Aktualisierungsprozess abgeschlossen war.

IGEL UMS Administrator Kommandozeilenschnittstelle

Die UMS Administrator Kommandozeilenschnittstelle ermöglicht es Ihnen, den IGEL UMS Administrator über ein Terminal zu steuern und Aktionen des UMS Administrator über Skripte zu automatisieren. Zu diesen Aktionen gehören das Erstellen und Bearbeiten von Datenbankverbindungen für den UMS-Server, das Sichern und Wiederherstellen der eingebetteten Datenbank, die Konfiguration von Kommunikationsports und Security, die Verwaltung der UMS-ID, die Konfiguration des Superusers und der Neustart des UMS-Servers.

Da diese Funktion eine vollständige Steuerung ohne grafische Desktop-Umgebung ermöglicht, kann die CLI-Anwendung auch auf Headless-Linux-Systemen ausgeführt werden.

Grundlegende Verwendung

Wie die grafische Anwendung des UMS Administrator erfordert auch die CLI erweiterte Rechte.

- Windows: Öffnen Sie eine Eingabeaufforderung (`cmd.exe`) als Administrator.
- Linux: Werden Sie `root` oder verwenden Sie `sudo`

Sie können das Hauptkommando `umsadmin-cli` von jedem Verzeichnis aus ausführen, da der Befehl auf dem `PATH` verfügbar ist.

- Um die globalen Optionen und die primären Unterkommandos zu sehen, geben Sie `umsadmin-cli` ein.

```
root@[redacted]:/home/ike/Downloads# umsadmin-cli -h
Usage: umsadmin-cli [-hV] [--machine-readable] [--no-header] [--quiet]
                    [--separator=<cliSeparator>] [COMMAND]
Configures UMS installation
  -h, --help              Show this help message and exit.
      --machine-readable  Prints output machine-readable with ';' as default
                            separator.
      --no-header         Do not print a header line.
      --quiet             Suppress all output to stdout/stderr.
      --separator=<cliSeparator>
                          Define custom column separator for CLI output.
  -V, --version           Print version information and exit.
Commands:
  db              Provides commands for database operations
  ports           Configuration of ports
  cipher          Manage cipher configuration.
  license         View and change licensing ID data
  token           Install network token vor UMS server or broker.
  su              Configuration of superuser
  restart-server  Restart the server
  help            Displays help information about the specified command
```

▶ Um alle möglichen Optionen für einen bestimmten Unterbefehl zu erhalten, geben Sie `umsadmin-cli` gefolgt von dem Unterbefehl ein, z.B. `umsadmin-cli db create`

```
root@td-                    :/home/ike# umsadmin-cli db create
Missing required options: '--type=TYPE', '--user=USER'
Usage: umsadmin-cli db create [-d=DOMAIN] [-H=HOST] [-I=INSTANCE] [-n=NAME]
                              [-p=PORT] [-S=SCHEMA] -t=TYPE -u=USER (-A |
                              (--password:file=<passwordFile> | --password:in))
Create a new database connection
  -A, --no-activate          Skip activation of database (no password required)
  -d, --domain=DOMAIN        The database domain
  -H, --host=HOST            The database host
  -I, --instance=INSTANCE    The database instance
  -n, --name=NAME            The database name
  -p, --port=PORT            The database port
      --password:file=<passwordFile>
                             Path to a file containing the password.
      --password:in          Shows an interactive prompt to enter the password.
  -S, --schema=SCHEMA        The database schema
  -t, --type=TYPE            The database type. Valid values:
                             embedded   -> Embedded DB
                             oracle     -> Oracle
                             oracle-rac -> Oracle RAC
                             mssql      -> SQL Server
```

ⓘ Bestimmte Unterbefehle haben keine Optionen und werden sofort ausgeführt. Bitte beachten Sie die Kommandoreferenz (see page 744).

▶ Um die komplette Online-Hilfe mit allen Befehlen zu erhalten, geben Sie `umsadmin-cli fullhelp` ein.

```
root@                    :/home/ike# umsadmin-cli fullhelp
Usage: umsadmin-cli [-hV] [--machine-readable] [--no-header] [--quiet]
                    [--separator=<cliSeparator>] [COMMAND]
Configures UMS installation
  -h, --help                Show this help message and exit.
      --machine-readable    Prints output machine-readable with ';' as default
                              separator.
      --no-header           Do not print a header line.
      --quiet               Suppress all output to stdout/stderr.
      --separator=<cliSeparator>
                            Define custom column separator for CLI output.
  -V, --version             Print version information and exit.
Commands:
db                          Provides commands for database operations

  help                      Displays help information about the specified command

  activate                  Activate a database connection
      -i  --id              The database identifier
          --password:file   Path to a file containing the password.
          --password:in     Shows an interactive prompt to enter the password.
```

▶ Um die Liste der verfügbaren Befehle zu erhalten, geben Sie `umsadmin-cli help`

```
C:\Program Files\IGEL\RemoteManager\rmadmin>umsadmin-cli help
Usage: umsadmin-cli [-hV] [--machine-readable] [--no-header] [--quiet]
                    [--separator=<cliSeparator>] [COMMAND]
UMS Administrator CLI to configure UMS installation
  -h, --help                Show this help message and exit.
      --machine-readable    Prints output machine-readable with ';' as default
                              separator.
      --no-header           Do not print a header line.
      --quiet               Suppress all output to stdout/stderr.
      --separator=<cliSeparator>
                            Define custom column separator for CLI output.
  -V, --version             Print version information and exit.
Commands:
  db              Provides commands for database operations
  ports           Configuration of ports
  cipher          Manage cipher configuration.
  licensing       View and change UMS ID data
  token           Install network token for UMS server or broker.
  su              Configuration of superuser
  restart-server  Restart the UMS server (deprecated, use 'server restart')
  server          Change the server run state
  reset-certs     Reset the web certificates
  ums-cluster     Set UMS cluster FQDN
  web-certs       Provides commands for web certificates configuration
  help            Displays help information about the specified command
  fullhelp        Show full help with all commands
```

▶ Um Hilfeinformationen zu einem beliebigen Befehl anzuzeigen, verwenden Sie `help` als Unterbefehl. Zum beispiel, geben Sie `umsadmin-cli web-certs help`

Globale Optionen

Wenn Sie die UMS Administrator CLI in einem Skript verwenden wollen, sollten Sie die Ausgabe nach stdout/stderr konfigurieren. Dies erleichtert die Weiterverarbeitung der Ausgabe von `umsadmin-cli` und die Extraktion aller relevanten Daten.

Bitte beachten Sie die unten aufgeführten Optionen.

--machine-readable

Maschinenlesbare Ausgabe mit einem Semikolon (;) als Standardtrennzeichen.

Beispiel:

```
root@machine:/home/locadmin# umsadmin-cli --machine-readable db list
ACTIVE;DATABASE;HOST;USER;DB-TYPE;ID
true;rmdb;localhost;root;Embedded DB;1
```

--no-header

Es wird keine Header-Zeile ausgegeben. Nicht alle Kommandos geben eine Header-Zeile aus.)

Beispiel:

```
root@machine:/home/locadmin# umsadmin-cli --machine-readable --no-header db
list
true;rmdb;localhost;root;Embedded DB;1
```

--quiet

Alle Ausgaben in stdout/stderr werden für einige Befehle unterdrückt, deren Ausführung lange dauern kann. Dies sind z. B. `db backup`, `db restore`, `db copy` und `server-restart`.

Beispiel:

```
root@machine:/home/locadmin# umsadmin-cli --quiet db backup -o /tmp/
mybackup02.pbak --full
root@machine:/home/locadmin#
```

Es ist wetierhin möglich, alle Ausgaben mit Betriebssystemfunktionen auf das Null-Device umzuleiten. Um zum Beispiel unter Linux die Standard- und Fehlerausgabe auf das Null-Device umzuleiten, verwenden Sie:

```
command … >/dev/null 2>&1
```

--separator

Definiert ein benutzerdefiniertes Spaltentrennzeichen für die Ausgabe in stdout/stderr.

Beispiel:

```
root@machine:/home/locadmin# umsadmin-cli --machine-readable --no-header --separator "||" db list
true||rmdb||localhost||root||Embedded DB||1
```

> Einige Trennzeichen, wie z. B. das Pipe-Symbol (|), müssen in Anführungszeichen gesetzt werden, da sie in Terminals besondere Funktionen haben.

Exit-Codes

Exit-Code	Bedeutung
0	Erfolgreiche Ausführung
1	Interner Fehler. Eine Fehlernummer wird auf stderr ausgegeben; für Details, siehe Fehlernummern (see page 778).
2	Falsche Verwendung der CLI oder ungültige Argumente

Kommandoreferenz

> **Allgemeine Verwendung der Passwortoptionen**
>
> Einige Befehle erfordern ein Passwort. Die Eingabe des Passworts im Klartext auf der Befehlszeile ist nicht sicher und daher nicht möglich. Daher muss eine der folgenden Passwortoptionen verwendet werden:
> `--password:in` zur interaktiven Eingabe des Passworts (eventuell mit Bestätigung)
> `--password:file <FILE>` für die Bereitstellung einer Datei, die das Passwort enthält
> Eine Passwortdatei muss das Passwort in der ersten Zeile enthalten, und die Passwörter dürfen nicht aus reinen Leerzeichen bestehen. Zusätzliche Zeilen mit Inhalt sind erlaubt, werden aber nicht ausgewertet.

> **Neustart des UMS Servers erforderlich**
>
> Die meisten der Befehle in den Abschnitten "Ports", "Cipher", "Reset Certificates" und "Superuser" ändern die UMS-Konfiguration und ein Neustart des UMS-Servers ist erforderlich, damit die neuen Einstellungen wirksam werden. Dies kann auf zwei Arten geschehen:
>
> - Verwenden Sie die entsprechende Funktion des Betriebssystems (z. B. `systemctl` unter Linux)
> - Verwenden Sie das Kommando `umsadmin-cli server restart`

Datenbank

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option	Anmerkungen
Alle konfigurierten Datenquellen auflisten	`db`	`list`					Zeigt die ID der Datenquelle an, die von anderen Kommandos benötigt wird. Die niedrigste ID ist 1. Die IDs können sich bei der Erstellung und Löschung von Datenquellen ändern.. Es wird dringend empfohlen, die ID immer zu extrahieren, bevor sie in anderen Befehlen mit `--id` verwendet wird Die ID wird wie folgt berechnet: höchste vorhandene ID + 1

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option	Anmerkungen
Alle Details einer Datenbank anzeigen	`db`	`show`	`-i`	`--id`	integer	Die ID der anzuzeigenden Datenbank	Führen Sie `umsadmin-cli db list` aus, um eine Liste der aktuellen Datenquellen zu erhalten und wählen Sie die ID einer Datenquelle aus. Führen Sie `umsadmin-cli db show --id <ID>` mit dieser ID aus.

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option	Anmerkungen
Erstellen Sie eine neue Datenbankverbindung	`db`	`create`	`-t`	`--type`	string	Der Datenbanktyp. Für eine Liste der möglichen Werte, geben Sie `umsadmin-cli db create` ein.	Typ, Benutzer und Port sind erforderlich. Andere Optionen können je nach DB-Typ erforderlich sein oder nicht `db create` aktiviert die Datenbank standardmäßig; dies kann durch die Verwendung von `-A` oder `--no-activate` verhindert werden. Eine Passwortoption kann dann nicht verwendet werden. Wenn die Aktivierung fehlschlägt, ist der Datenquelleneintrag noch vorhanden und nicht aktiv (gleiches Verhalten wie im grafischen UMS Administrator).

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option	Anmerkungen
							'rmdb' ist ein reservierter Name für den eingebetteten Datenbanktyp und kann nicht für andere Typen verwendet werden.
			`-H`	`--host`	string	Datenbank-Host	
			`-d`	`--domain`	string	Datenbank-Domäne	
			`-p`	`--port`	integer	Datenbank-Port	
			`-u`	`--user`	string	Benutzer für die Datenbank	
			`-S`	`--schema`	string	Schema der Datenbank	
			`-n`	`--name`	string	Name der Datenbank. Freier Text, außer 'rmdb'; dieser Name ist für die eingebettete Datenbank reserviert.	

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option	Anmerkungen
			`-I`	`--instance`	string	Name der Datenbankinstanz	
			`-A`	`--no-activate`		Die Datenbank wird nicht aktiviert.	
				`--password:file`	string	Das Passwort wird aus einer Datei (Klartext) gelesen, deren Pfad nach dieser Option angegeben wird.	
				`--password:in`	string	Das Passwort wird von stdin gelesen; eine interaktive Eingabeaufforderung wird angezeigt.	

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option	Anmerkungen
Bearbeiten einer Datenquelle	`db`	`edit`	`-t`	`--type`	string	Datenbanktyp. Für eine Liste der möglichen Werte geben Sie `umsadmin-cli db create` ein.	Embedded-Datenbanken können nicht bearbeitet werden (wie im grafischen UMS Administrator). Alle Optionen außer `--id` sind optional.
			`-H`	`--host`	string	Datenbank-Host	
			`-d`	`--domain`	string	Datenbank-Domäne	
			`-i`	`--id`	integer	ID der zu bearbeitenden Datenbank	
			`-I`	`--instance`	string	Name der Datenbankinstanz	

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option	Anmerkungen
				`--jdbc-params`	string	Zusätzlicher JDBC-Parameter	Einzelheiten zu den JDBC-Parametern finden Sie unter Wie kann ich eine Datenquelle im IGEL UMS Administrator einrichten? (see page 730) Beispiele:

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option	Anmerkungen
							• `rmadmin\umsadmin-cli.exe db create --type=mssql --name=rmdb12_00 --host=122.30.229.1 --port=1433 --user=rmdb --password:in --jdbc-params sendStringParameterSAsUnicode=false;` • `rmadmin/umsadmin-cli.bin db edit -i 1 --jdbc-params sendStringParameterSAsUnicode=false;`

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option	Anmerkungen
			`-n`	`--name`	string	Der Name der Datenbank. Freier Text, außer 'rmdb'; dieser Name ist für die Embedded-Datenbank reserviert.	
			`-p`	`--port`	integer	Datenbank-Port	
			`-S`	`--schema`	string	Schema der Datenbank	
			`-u`	`--user`	string	Benutzer für die Datenbank	

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option	Anmerkungen
Datenbankverbindung aktivieren	`db`	`activate`		`--password:file`	string	Das Passwort wird aus einer Datei (Klartext) gelesen, deren Pfad nach dieser Option angegeben wird. Biespiel: `umsadmin-cli db activate --password:file /home/ike/password.txt`	
				`--password:in`	string	Das Passwort wird von stdin gelesen; eine interaktive Eingabeaufforderung wird angezeigt.	
			`-i`	`--id`	integer	ID der zu aktivierenden Datenbank	

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option	Anmerkungen
Aktive Datenbankverbindung aktivieren	`db`	`deactivate`	`-i`	`--id`	integer	ID der zu deaktivierenden Datenbank	
Aktive Datenbankverbindung testen	`db`	`test`		`--password:file`	string	Das Passwort wird aus einer Datei (Klartext) gelesen, deren Pfad nach dieser Option angegeben wird. Beispiel: `umsadmin-cli db test --password:file /home/ike/password.txt`	
				`--password:in`	string	Das Passwort wird von stdin gelesen; eine interaktive Eingabeaufforderung wird angezeigt.	

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option	Anmerkungen
Aktive Datenbank optimieren	`db`	`optimize`					Dieser Befehl kann nur auf eine Embedded-Datenbank oder eine Derby-Datenbank angewendet werden.
Kopie der aktuellen Datenbank anlegen	`db`	`copy`	`-t`	`--target`	integer	ID der Ziel-Datenbank Um die Datenbank-ID zu erhalten, geben Sie `umsadmin-cli db list` ein	
				`--password:file`	string	Das Passwort wird aus einer Datei (Klartext) gelesen, deren Pfad nach dieser Option angegeben wird.	
				`--password:in`	string	Das Passwort wird aus einer Datei (Klartext) gelesen, deren Pfad nach dieser Option angegeben wird.	

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option	Anmerkungen
Datenbankverbindung löschen	`db`	`delete`	`-i`	`--id`	integer	ID der Datenbankverbindung, die gelöscht werden soll	
Sicherungskopie der aktuellen Embedded-Datenbank erstellen	`db`	`backup`	`-o`	`--outfile`		Pfad zur Zieldatei. Die Dateiendung `.pbak` wird automatisch hinzugefügt. Vorhandene Sicherungsdateien werden nicht überschrieben.	
			`-f`	`--full`		Vollständige Sicherung. Datenbank, Serverkonfigurationen und Übertragungsdateien sind enthalten.	

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option	Anmerkungen
			`-p`	`--parent`		Alle Verzeichnisse für den angegebenen Pfad werden erstellt, sofern sie nicht bereits vorhanden sind.	
Sicherungskopie in die Embedded-Datenbank wiederherstellen	`db`	`restore`	`-f`	`--file`		Pfad zur Sicherungsdatei	

Ports

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option
Alle Ports und SSL-only-Flag anzeigen	`ports`	`list`				

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option
Neue Portnummern oder SSL-only-Flag setzen	`ports`	`set`	`-d`	`--dev-comm`	integer	Port für die Kommunikation mit den Geräten. Einzelheiten siehe Geräte kontaktieren die UMS (see page 32).
			`-j`	`--java-webstart`	integer	Port für Java Web Start
			`-w`	`--web-server`	integer	Port für den UMS Server. Einzelheiten siehe UMS mit interner Datenbank (see page 24) und UMS mit externer Datenbank (see page 25).
			`-e`	`--embedded`	integer	Port der Embedded-Datenbank
				`--ssl-only`	boolean	Nur SSL-Verbindungen erlauben

Cipher

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option
Alle Ciphers auflisten, optional gefiltert	`cipher`	`list`				Alle Ciphers auflisten
			`-e`	`--enabled`		Nur aktivierte Ciphers auflisten

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option
			`-d`	`--disabled`		Nur deaktivierte Ciphers auflisten
Ciphers aktivieren	`cipher`	`enable`				Ciphers aktivieren. Die Ciphers werden durch Leerzeichen getrennt. Beispiel: `umsadmin-cli cipher enable CIPHER1 CIPHER 2 CIPHER3`
				`--all`		Auf alle anwenden; einzelne Ciphernamen werden ignoriert.
Ciphers deaktivieren	`cipher`	`disable`				Ciphers deaktivieren. Die Ciphers werden durch Leerzeichen getrennt. Beispiel: `umsadmin-cli cipher disable CIPHER1 CIPHER 2 CIPHER3`
				`--all`		Auf alle anwenden; einzelne Ciphernamen werden ignoriert..

Web-Zertifikate

Aktion	Primäres Unterkommando	Sekundäres Unterkommando	Kurze Option	Lange Option	Beschreibung der Option	
Web-Zertifikate zurücksetzen	`reset-certs`		`-y`	`--yes`	Der Reset wird erst nach Bestätigung ausgeführt	
Zeigt Hilfeinformationen über den angegebenen Befehl an	`web-certs`	`help`				
Zertifikat dem aktuellen oder allen Servern zuweisen	`web-certs`	`assign-cert`	`-f`	`--fingerprint-sha1`	SHA1-Fingerabdruck des Zertifikats	

Aktion	Primäres Unterkommando	Sekundäres Unterkommando	Kurze Option	Lange Option	Beschreibung der Option	
			`-s`	`--server`	Server, dem das Zertifikat zugewiesen ist. Mögliche Werte: • `ALL_SERVER` • `CURRENT_SERVER` (standard)	
Stammzertifikat erstellen	`web-certs`	`create-root-cert`	`-a`	`--algorithm`	Schlüsselpaar-Algorithmus; `rsa` oder `ec` (standard: `rsa`)	
			`-c`	`--country`	Ländercode (zwei Buchstaben)	
			`-d`	`--expiration-date`	Verfallsdatum (YYYY-MM-DD) (Aktuelles Datum plus 20 Jahre, falls nicht angegeben.)	

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Beschreibung der Option	
				`--key-size`	Schlüsselgröße (4096, 8192, ... bits). Mögliche Werte: • 4k (default) • 8k • 12k • 16k	
			`-l`	`--locality`	Standort (Wenn nicht angegeben, wird der Hash-Code einer zufälligen uuid verwendet).	
			`-n`	`--name`	Name des Zertifikats (Standard: Root certificate)	
				`--named-curve`	Named curve Gültige Werte: • `nist-p-384` (default) • `nist-p-256` • `nist-p-521`	

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Beschreibung der Option	
			`-o`	`--organization`	Organisation (obligatorisch)	
Signiertes Zertifikat erstellen	`web-certs`	`create-signed-cert`	`-f`	`--fingerprint-sha1`	SHA1-Fingerabdruck des übergeordneten CA-Zertifikats	Das übergeordnete CA-Zertifikat wird durch den SHA1-Fingerabdruck angegeben. Es spielt keine Rolle, ob Sie kein Trennzeichen, '-' oder ':' als Trennzeichen für den Fingerabdruck verwenden.
			`-n`	`--name`	Name des Zertifikats (Standard: Certificate)	
				`--cn`	Common name	
			`-c`	`--country`	Ländercode (zwei Buchstaben)	

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Beschreibung der Option	
			`-o`	`--organization`	Organisation	
			`-l`	`--locality`	Standort (Wenn nicht angegeben, wird der Hash-Code einer zufälligen uuid verwendet).	
			`-d`	`--expiration-date`	Verfallsdatum (YYYY-MM-DD) (Aktuelles Datum plus 1 Jahr, falls nicht angegeben.)	
				`--ca`	Typ des Zertifikats: • `true` = CA certificate • `false` = End entity (standard)	

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Beschreibung der Option	
			`-h`	`--hostname`	Hostname oder einer der folgenden Werte: • ALL_SERVER • CURRENT_SERVER (default)	Sie können eine Liste von Hostnamen für den Subject Alternative Name (SAN) angeben oder Sie können angeben, ob der aktuelle Server (CURRENT_SERVER) oder alle Server (ALL_SERVER) in der SAN-Liste aufgeführt werden.
Zertifikat löschen	`web-certs`	`delete`	`-f`	`--fingerprint-sha1`	SHA1-Fingerprint des Zertifikats	
Zertifikat exportieren	`web-certs`	`export-cert`	`-c`	`--cert-file`	Pfad, in den das Zertifikat exportiert werden soll (Der Name `cert.cert` wird verwendet, wenn nur ein Verzeichnis angegeben ist.)	

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Beschreibung der Option	
			`-f`	`--fingerprint-sha1`	SHA1-Fingerabdruck des Zertifikats	
Zertifikatskette in Schlüsselspeicher exportieren (JKS)	`web-certs`	`export-cert-chain`	`-f`	`--fingerprint-sha1`	SHA1-Fingerabdruck des Zertifikats	
			`-k`	`--keystore-file`	Pfad zum Keystore, in den die Zertifikatskette exportiert werden soll	
				`--password:file`	Pfad zu einer Datei, die das Kennwort enthält	

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Beschreibung der Option	
				`--password:in`	Zeigt eine interaktive Aufforderung zur Eingabe des Passworts	
Zertifikatskette aus Keystore importieren	`web-certs`	`import-cert-chain`	`-k`	`--keystore-file`	Die Keystore-Datei	
				`--password:file`	Pfad zu einer Datei, die das Kennwort enthält	
				`--password:in`	Zeigt eine interaktive Aufforderung zur Eingabe des Passworts	

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Beschreibung der Option	
Entschlüsselten privaten Schlüssel importieren	`web-certs`	`import-private-key`	`-f`	`--fingerprint-sha1`	SHA1-Fingerabdruck des übergeordneten CA-Zertifikats	
			`-p`	`--private-key-file`	Die Datei, die den privaten Schlüssel enthält	
Stammzertifikat importieren	`web-certs`	`import-root-cert`	`-c`	`--cert-file`	Das Stammzertifikat `(CERT, CER, CRT, PEM)`	
Signiertes Zertifikat importieren	`web-certs`	`import-signed-cert`	`-c`	`--cert-file`	Das Stammzertifikat (`CERT, CER, CRT, PEM`)	Ein Zertifikat kann nur importiert werden, wenn kein anderes Zertifikat mit demselben Fingerabdruck bereits existiert, sonst erhalten Sie eine Fehlermeldung.

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Beschreibung der Option	
			`-f`	`--fingerprint-sha1`	SHA1 fingerprint des übergeordneten CA-Zertifikats	
Den zugewiesenen Server eines Zertifikats auflisten	`web-certs`	`list-assigned-server`	`-f`	`--fingerprint-sha1`	SHA1-Fingerabdruck des Zertifikats	
Alle Webzertifikate oder Details zu einem Zertifikat auflisten	`web-certs`	`list`	`-f`	`--fingerprint-sha1`	SHA1-Fingerabdruck des Zertifikats	Wenn Sie einen Fingerabdruck angeben, werden die Details des Zertifikats mit diesem Fingerabdruck angezeigt.

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Beschreibung der Option	
Zertifikat erneuern	`web-certs`	`renew-cert`	`-f`	`--fingerprint-sha1`	SHA1-Fingerabdruck des Zertifikats	Sie müssen nur den Fingerabdruck des Zertifikats angeben, das erneuert werden soll. Wenn die anderen Parameter nicht angegeben werden, werden die Werte des alten Zertifikats verwendet (mit neuem Ablaufdatum).
			`-n`	`--name`	Name des Zertifikats	
				`--cn`	Common name	
			`-c`	`--country`	Ländercode (zwei Buchstaben)	
			`-o`	`--organization`	Organisation	
			`-l`	`--locality`	Standort	

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Beschreibung der Option	
			`-d`	`--expiration-date`	Verfallsdatum (YYYY-MM-DD) (Aktuelles Datum plus 1 Jahr, falls nicht angegeben.)	
			`-h`	`--hostname`	Hostname oder einer der folgenden Werte: • `ALL_SERVER` • `CURRENT_SERVER`	

Superuser

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option
UMS Superuser anzeigen	`su`	`list`				

Aktion	Primäres Unterkommando	Sekundäres Unterkommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option
UMS Superuser ändern	`su`	`change`	`-u`	`--user`	string	Neuer Superuser
			`-p`	`--password:file`	string	Das Passwort wird aus einer Datei (Klartext) gelesen, deren Pfad nach dieser Option angegeben wird.
				`--password:in`	string	Das Passwort wird von stdin gelesen; eine interaktive Eingabeaufforderung wird angezeigt.

UMS-ID

Aktion	Primäres Unterkommando	Sekundäres Unterkommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option
Aktuelle UMS-IDs anzeigen	`licensing`	`list`				
Neue UMS-ID erstellen	`licensing`	`create`				
UMS-ID sichern	`licensing`	`backup`	`-o`	`--outfile`	string	Pfad zur Zieldatei (Dateiendung: `.ksbak`)

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option
			`-p`	`--parent`		Alle Verzeichnisse für den angegebenen Pfad werden erstellt, sofern sie nicht bereits vorhanden sind.
				`--password:file`	string	Das Passwort wird aus einer Datei (Klartext) gelesen, deren Pfad nach dieser Option angegeben wird.
				`--password:in`	string	Das Passwort wird von stdin gelesen; eine interaktive Eingabeaufforderung wird angezeigt.
UMS-ID aus einem Backup wiederherstellen	`licensing`	`restore`	`-f`	`--file`	string	Pfad zur Backupdatei
				`--password:file`	string	Das Passwort wird aus einer Datei (Klartext) gelesen, deren Pfad nach dieser Option angegeben wird.
				`--password:in`	string	Das Passwort wird von stdin gelesen; eine interaktive Eingabeaufforderung wird angezeigtaus einer Datei (Klartext), deren Pfad nach dieser Option angegeben wird.

Netzwerktoken

Aktion	Primäres Unterkommando	Kurze Option	Lange Option	Werttyp	Beschreibung der Option	Anmerkungen
Netzwerk-Token für den UMS Server oder einen Broker installieren	`token`	`-f`	`--token-file`	string	Pfad zur Datei des Tokens	Dieser Befehl ist auch als eigenständiger Befehl namens `umstokeninstall-cli` in reinen Broker-Installationen verfügbar. Er ist äquivalent zu `umsadmin-cli token`.
			`--server`	boolean	Token für UMS Server installieren	
			`--broker`	boolean	Token für Broker installieren	

UMS Cluster

Aktion	Primäres Unterkommando	Sekundäres Unterkommando	Kurze Option	Lange Option	Beschreibung der Option
Den aktuellen FQDN des UMS Clusters anzeigen	`ums-cluster`	`list`			

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Beschreibung der Option
Einen neuen FQDN für den UMS Cluster festlegen	`ums-cluster`	`create`	`-n`	`--name`	Name für den neuen FQDN des UMS Clusters
Den aktuellen FQDN des UMS Clusters löschen	`ums-cluster`	`remove`			

Server

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Beschreibung der Option
Lokalen UMS Server starten	`server`	`start`			
Lokalen UMS Server stoppen	`server`	`stop`			
Lokalen UMS Server neu starten	`server`	`restart`			
Update-Modus für den lokalen UMS Server beenden	`server`	`end-update-mode`			

Aktion	Primäres Unter-kommando	Sekundäres Unter-kommando	Kurze Option	Lange Option	Beschreibung der Option
Distributed-Modus (see page 246) der UMS Installation einstellen	`server`	`distributed`	`-e`	`--enable`	Distributed UMS aktivieren
			`-d`	`--disable`	Distributed UMS deaktivieren

Fehlernummern

Die Fehlernummern werden in folgendem Format ausgegeben:

```
<E-NNNN>: <HUMAN READABLE MESSAGE>
```

Einige Fehlerbeschreibungen in der folgenden Tabelle enthalten die Phrase "[param]". Diese wird zur Laufzeit durch Angaben zum jeweiligen Fehler ersetzt, z.B. den problematischen Pfad für E-1030.

Error number	Error description
1000	Unable to connect to database. UMS server may be down.
1001	Cannot get database configurations.
1002	Cannot create database.
1003	Cannot activate database. [param]
1004	Internal error while activating database.
1005	Database already exists in this configuration.
1006	Database type is unknown.
1007	Database is already activated.
1008	Cannot edit database configurations.
1009	Internal error while optimizing database.
1010	The active data source type is not Embedded or Derby and does not support optimization.
1011	Test of the active data source failed.
1012	No database is activated.
1013	Cannot deactivate database.
1014	No database is active or the active database is not of type 'Embedded' or 'Derby'.
1020	Database could not be deleted.
1030	The specified directory for the backup does not exist: [param]
1031	Internal error while attempting database backup.
1040	The specified backup file was not found.
1041	The specified backup file has an invalid file type.
1042	Unable to read the specified backup file.

Error number	Error description
1043	Internal error while activating data source after restore.
1044	Internal error while attempting to restore database.
1045	The active data source is not embedded or there is no active data source.
1051	Authentication error or internal error when an attempt was made to copy the database
1052	Error Accessing credentials of source database
1090	A name is required for non-embedded database types.
1091	Activation failed, incorrect password provided.
1092	Backup failed, the specified file already exists.
1093	Port number is required for non-Embedded database.
1094	A data source of the Embedded type cannot be edited.
1095	No such data source with this ID.
1100	The name 'rmdb' is reserved for the Embedded database.
2000	Internal error while reading port configuration.
2001	Internal error while setting port configuration.
2002	Internal error while restarting UMS server.
2003	Invalid port number provided.
2004	Port number [param] already configured.
3000	Internal error while reading cipher data.
3001	Internal error while changing cipher configuration.
3002	Invalid ciphers provided: [param]
4000	Resetting web certificates requires '--yes' option for confirmation.
4001	Internal error while resetting web certificates.
5000	Internal error while reading superuser credentials.
5001	Internal error while writing superuser credentials.
5002	No username was provided for new credentials.

Error number	Error description
5003	Unable to set superuser credentials. There is no active data source.
6000	Unable to create a new UMS ID.
6001	The specified file for the license key backup already exists.
6002	No internal license keystore found.
6003	Internal error while creating license key backup.
6004	Internal error while restoring license key backup.
6005	The specified file for the license key backup does not exist.
6006	The specified password for the license key backup is incorrect.
6007	The specified path for the license key backup does not exist: [param]
7000	Token file was not found.
7001	Setup type not defined, token not installed.
7501	Unable to set UMS cluster FQDN.
7502	Unable to show UMS cluster FQDN.
7503	Unable to delete the cluster FQDN.
8000	Internal error while restarting the UMS server.
8001	Internal error while starting the UMS server.
8002	Internal error while stopping the UMS server.
8003	Internal error while ending the update mode of the UMS Server.
8004	Internal error while setting the distributed mode of the UMS installation.
8005	Either --enable or --disable must be provided in the options.
8006	Distributed UMS not recommended for Derby Embedded Database.
9000	An error with the password file occurred: [param]
9001	The provided passwords did not match. Aborted.

Error number	Error description
9002	The provided password exceeds the maximum character limit ([param]) or contains only whitespace.
9700	File [param] doesn't exist!
9701	Keystore contains no certificate entries!
9702	Keystore password is invalid!
9703	Keystore couldn't be read!
9704	Could not import certificate chain!
9705	Internal error while importing certificate chain!
9706	No SHA1 fingerprint specified!
9707	Could not delete certificate(s) with SHA1 fingerprint [param]!
9708	Certificate must not be deleted because it is currently in use!
9709	Root certificate creation failed!
9710	Certificate could not be created! Private key of CA certificate is not known.
9711	Certificate could not be created! CA certificate is not valid.
9712	Could not find CA certificate with specified fingerprint.
9713	Certificate could not be created! CA certificate does not meet the requirements.
9714	Certificate could not be created! Requirements for CA certificate creation are not met.
9715	Creation of signed certificate failed!
9716	Certificate could not be created! Certificate name too long (only 200 characters are allowed)!
9717	Could not find certificate with specified fingerprint!
9718	Certificate could not be renewed! Certificate has no CA parent.
9719	Certificate file [param] doesn't exist!
9720	Certificate is invalid!
9721	Import of certificate failed! No CA certificate.
9722	Import of certificate failed!

Error number	Error description
9723	Import of certificate failed! Certificate is not valid.
9724	Import failed! Certificate doesn't contain any subject alternative names.
9725	Import of private key failed! File [param] doesn't exist.
9726	Import of private key failed! Private key is encrypted. Decrypt it before importing it.
9727	Import of private key failed!
9728	Certificate already has private key!
9729	Import of private key failed! Private key does not match the specified certificate.
9730	Export of certificate failed! Directory [param] doesn't exist.
9731	Export of certificate failed!
9732	Export of certificate chain failed! Directory [param] doesn't exist.
9733	Certificate must not be a root or CA certificate!
9734	Export of certificate chain failed!
9735	Password must be at least 6 characters long!
9736	Assignment of certificate failed!
9737	Private key is not known!
9738	Could not read certificate info!
9739	Import failed! Certificate with same fingerprint already exists.
9740	Import failed! No valid root certificate.
9741	Import failed! Verification of signature failed.
9742	Import failed! No valid CA certificate available.
9743	Could not read assigned server info!
9744	Could not find certificate with specified fingerprint or no server is assigned to certificate!
9745	Common name is invalid! Only A-Z, a-z, 0-9, - and . are allowed.

IGEL UMS Web App

Die IGEL Universal Management Suite (UMS) Web App ist eine webbasierte Benutzerschnittstelle zum UMS Server. Die Installation der UMS Web App erfolgt über den UMS Installer, siehe IGEL UMS Installation (see page 246).

⚠ Die UMS Web App kann derzeit nur zusätzlich zur Java-basierten UMS Konsole verwendet werden. Einige Funktionen sind momentan nur in der UMS Web App verfügbar, andere nur in der UMS Konsole; siehe die Feature-Matrix unter Überblick über die IGEL UMS (see page 238).
Der Funktionsumfang der UMS Web App wird ständig erweitert.
Alle Features, die bereits in der UMS Web App verfügbar sind, werden vollständig unterstützt.

Zu den Hauptmerkmalen der UMS Web App gehören:

- Verwaltung der Gerätekonfiguration und Erstellung von Profilen
- Spiegeln-Funktion für Geräte und diverse Gerätebefehle (Energiesteuerung, Update, Senden/Erhalten von Einstellungen, Zurücksetzung auf Werkseinstellungen usw.)
- Zuweisung von Objekten zu Geräten und Geräteverzeichnissen
- Import und Verwaltung von IGEL OS Apps und deren Versionen
- Überwachung des Status des UMS Netzwerks
- konfigurierbare Suchfunktionalität
- Protokollierung der Aktionen

ⓘ Wenn Sie mehr über die Nutzung der UMS Web App in IGEL COSMOS erfahren möchten, lesen Sie unseren Leitfaden Einstieg in IGEL COSMOS, oder schauen Sie sich den IGEL Academy Kurs "IGEL Certified Professional (ICP) for COSMOS" an:
https://learn.igel.com/learn/course/157/igel-certified-professional-icp-for-cosmos

Wichtige Informationen zur IGEL UMS Web App

Beachten Sie die folgenden Informationen zur IGEL Universal Management Suite (UMS) Web App.

Unterstützte Umgebung

- Die minimale unterstützte Auflösung ist 768 px.
  Wenn Sie die UMS Web App auf mobilen Geräten verwenden möchten, beachten Sie, dass die unterstützte Mindestbreite für das Responsive Design 768 px beträgt.
- Die Anforderungen an RAM und Speicherplatz finden Sie unter Installationsvoraussetzungen für die IGEL UMS (see page 250).

Installation

- Im Falle einer High Availability- oder Distributed UMS-Umgebung:
  - Die UMS Web App muss nicht unbedingt auf jedem UMS Server installiert sein. Wenn Sie sich jedoch dafür entscheiden, die Anwendung auf mehreren UMS Servern zu installieren, können Sie sie auf allen Servern verwenden. Die Daten werden synchronisiert.
  - Die UMS Konsole und die UMS Web App können auf verschiedenen Servern installiert sein.

Anmeldung

- Die Anmeldedaten des Datenbankbenutzers werden für die UMS Web App nicht akzeptiert. Wie Sie sich an der UMS Web App anmelden, finden Sie unter Wie kann ich mich an der IGEL UMS Web App anmelden? (see page 786)

Berechtigungen

- Die UMS Web App und die UMS Konsole verwenden die gleichen Berechtigungen. Detaillierte Informationen zu den Zugriffsrechten in der IGEL UMS finden Sie unter Administratorkonten und Zugriffsrechte (see page 676).
- Es gibt einige Berechtigungen, die nur für die UMS Web App gelten – **Logging-Einträge löschen**, **Massenhafte Geräte-Aktionen** und **App Management**. Sie können in der UMS Konsole unter **System > Administratorkonten > Neu / Bearbeiten > Allgemein - WebApp** gesetzt werden.
- Leseberechtigungen für ein Verzeichnis ermöglichen den Zugriff auf Geräte in diesem Verzeichnis; Berechtigungen nur für Geräte sind nicht ausreichend.
- Für die Zuweisung von Apps (Ausnahme: IGEL OS Base System) benötigen Sie die gleichen Berechtigungen wie für die Zuweisung von Profilen zu Geräten, siehe Objekte zuordnen (see page 691). Dies liegt daran, dass Nicht-Base-System-Apps den Geräten automatisch über Profile, die diese Apps konfigurieren, zugewiesen werden (sogenannte implizite App-Zuweisung).
- Für die Zuweisung von IGEL OS Base System ist die Berechtigung **Basissystem / Firmwareupdate zuordnen** erforderlich (unter **UMS Konsole > Geräte > [Kontextmenü des Geräts / Geräteverzeichnisses] > Berechtigungen** gesetzt).

- Die folgenden Berechtigungen sind erforderlich:
  - Rechte für den Knoten **Server-Netzwerkeinstellungen** unter **UMS Konsole > UMS Administration > Globale Konfiguration** für den Zugang zu
    - **UMS Web App > Apps > Einstellungen > App Portal**
    - **UMS Web App > Apps > Einstellungen > Automatische Updates**
    - **UMS Web App > Netzwerk > Einstellungen > Netzwerk > Alias des UMS Netzwerks**
  - Rechte für den Knoten **UMS Features** unter **UMS Konsole > UMS Administration > Globale Konfiguration** für den Zugang zu
    - **UMS Web App > Apps > Einstellungen > UMS as an Update Proxy**
    - **UMS Web App > Netzwerk > Einstellungen > UMS Features**

Synchronisierung zwischen der UMS Konsole und der UMS Web App

- Die UMS Web App und die UMS Konsole verwenden dieselbe Datenbank, dieselben Benutzerrechte und Zertifikate.
- In der UMS Konsole vorgenommene Änderungen sind sofort in der UMS Web App verfügbar und umgekehrt.
- Änderungen, die in der UMS Konsole vorgenommen werden, sind nicht sofort durchsuchbar, sondern erst nach dem nächsten Reindizieren, das stündlich durchgeführt wird.
- In der UMS Konsole vorgenommene Profileinstellungsänderungen sowie Einstellungen für die neu erstellten Profile werden in der UMS Web App unter **Konfiguration > [Profilname] > Aktivierte Einstellungen** nicht sofort angezeigt, sondern erst nach dem nächsten Reindizieren: dieses Reindizieren wird mit einem eintägigen Intervall durchgeführt.

Protokollieren

- Nicht alle Aktionen, die in der UMS Konsole durchgeführt werden, werden in der UMS Web App angezeigt. Protokolle der UMS Web App werden in der UMS Konsole nicht angezeigt
- Log-Dateien für die UMS Web App finden Sie auch in `/rmguiserver/logs/wums*`

Zertifikat

- Standardmäßig wird das vom UMS Server verwendete selbstsignierte Zertifikat von Browsern nicht akzeptiert und eine Sicherheitswarnung wird angezeigt. Wie Sie das Problem lösen können, finden Sie unter UMS Web App: The Browser Displays a Security Warning (Certificate Error) (see page 174).

Massenaktionen

- Derzeit ist es nicht möglich, gleichzeitig mehrere Geräte oder Verzeichnisse auszuwählen. Wenn Sie Befehle massenweise ausführen wollen, können Sie dies jetzt nur durch Auswahl eines einzelnen Verzeichnisses tun.

Wie kann ich mich an der IGEL UMS Web App anmelden?

Der folgende Artikel beschreibt, wie Sie die IGEL Universal Management Suite (UMS) Web App öffnen und mit welchen Zugangsdaten Sie sich anmelden können. Einen kurzen Überblick über die UMS Web App finden Sie unter IGEL UMS Web App (see page 783).

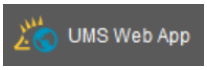
Auf die UMS Web App zugreifen

So öffnen Sie die UMS Web App:

▶ Geben Sie im Browser folgende URL ein: URL `https://<server>:8443/webapp/#/login`.[36]

⚠ "8443" ist der standardmäßigen GUI-Serverport, siehe "GUI-Serverport" unter Einstellungen - Servereinstellungen im IGEL UMS Administrator ändern (see page 709). Ausführliche Informationen zu den UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).
Wenn Sie den Port des GUI-Servers geändert haben, passen Sie die URL entsprechend an.

ODER

▶ Klicken Sie in der Symbolleiste der UMS Konsole auf das Symbol 

.

Anmeldedaten für die UMS Web App

Um sich in die UMS Web App einzuloggen, können Sie die folgenden Daten verwenden:

- Die Anmeldedaten des UMS Superusers, die unter **UMS Administrator > Datenquelle > UMS Superuser** geändert werdend können. Siehe UMS Superuser ändern (see page 737).
- Das zusätzlich erstellte Administratorkonto, das unter **UMS Konsole > System > Administratorkonten** hinzugefügt werden kann. Siehe Administratorkonten und Zugriffsrechte (see page 676).

⚠ Die Anmeldedaten des Datenbankbenutzers werden für die UMS Web App nicht akzeptiert.

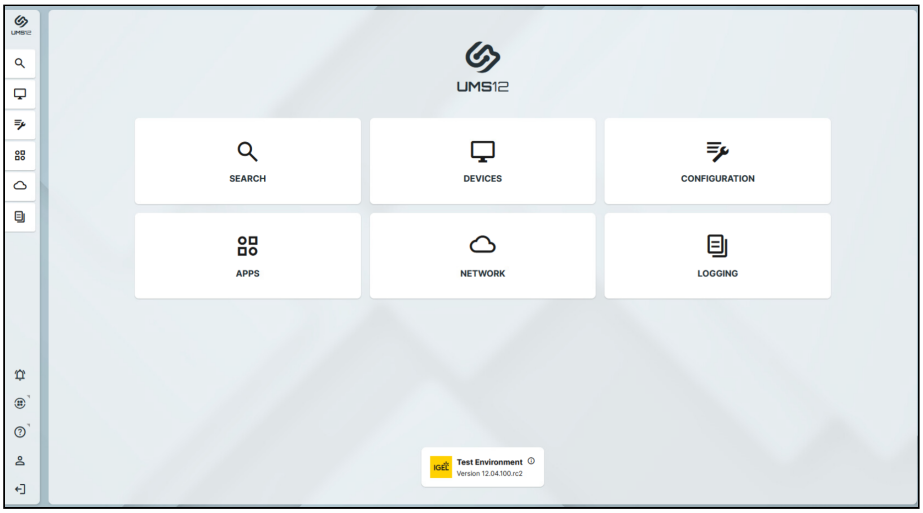
ⓘ UMS Web App bietet einen Brute-Force-Schutz:
- Nach einigen fehlgeschlagenen Anmeldeversuchen wird das Benutzerkonto temporär gesperrt. Dies gilt auch für Konten, die nicht existieren.
- Um das Sondieren zu verhindern, wird eine dynamische Anmeldeverzögerung (Millisekunden) implementiert. Dies ist erforderlich, da die Antwortzeit ein Indikator für die (Nicht-)Existenz eines Kontos sein könnte.

36 https://localhost:8443/webapp.

IGEL UMS Web App User Interface

Der folgende Artikel beschreibt die Benutzeroberfläche der IGEL Universal Management Suite (UMS) Web App, die mit der IGEL UMS Version 12.03.100 eingeführt wurde.

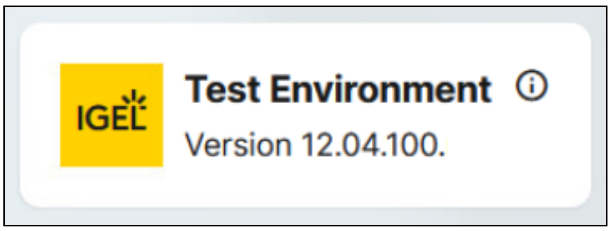
Startseite



▶ Klicken Sie auf die Kacheln oder die entsprechenden Schaltflächen in der Seitenleiste, um einen Bereich aufzurufen. Weitere Informationen zu jedem Bereich finden Sie unter:

- Geräte - Ihre Endgeräte in der IGEL UMS Web App ansehen und verwalten (see page 799)
- Konfiguration - Zentralisierte Verwaltung von Geräteeinstellungen in der IGEL UMS Web App (see page 828)
- Apps - Import und Konfiguration von Apps für IGEL OS 12-Geräte über die UMS Web App (see page 862)
- Netzwerk-Einstellungen in der IGEL UMS Web App (see page 897)
- Logging in der IGEL UMS Web App (see page 903)
- Suche nach Geräten in der IGEL UMS Web App (see page 792)

System Info Box



Die Infobox am unteren Rand der Startseite zeigt Versionsinformationen zu Ihrem IGEL UMS an. Falls angegeben, wird hier auch der Spitzname Ihres UMS angezeigt; siehe Netzwerk-Einstellungen in der IGEL UMS Web App (see page 897).
Das gleiche Informationsfeld wird auch in den meisten anderen Bereichen angezeigt.

▶ Klicken Sie auf ⓘ um weitere Details anzuzeigen.

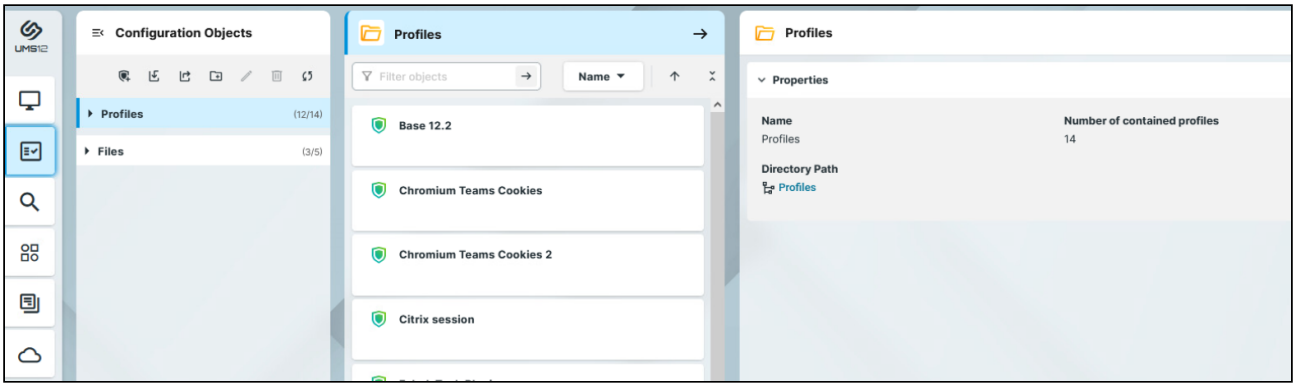
Schaltflächen der Seitenleiste

	Bringt Sie zurück zur Startseite.
	Unter **Nachrichten** können Sie den aktuellen Status und die Ergebnisse der Gerätebefehle und anderer Aktionen wie dem Import von IGEL OS Apps etc. einsehen. ⓘ Die Nachrichten werden beim erneuten Laden der UMS Web App Seite im Browser automatisch gelöscht. ▶ Klicken Sie auf eine Nachricht, um Details anzuzeigen. • Ein erfolgreich ausgeführter Befehl wird mit ✓. • Ein fehlgeschlagener Befehl wird durch ein Warnsymbol gekennzeichnet ⚠. • Ein teilweise fehlgeschlagener Befehl wird mit einem Warnsymbol gekennzeichnet ⚠.
	Direkter Link zum IGEL App Portal. Der Link wird in einer neuen Browser-Registerkarte geöffnet.

	Direkter Link zur UMS Web App Dokumentation auf kb.igel.com[37]. Der Link wird in einer neuen Browser-Registerkarte geöffnet.
	Unter **Anpassen** können Sie die Sprache der IGEL UMS Web App einstellen und das Erscheinungsbild in den **dunklen Modus** oder **hellen Modus** ändern.
	Abmelden von der UMS Web App

Layout

In den Bereichen **Geräte**, **Konfiguration**, **Suche**, **Netzwerk** und **Apps** ist die Oberfläche in einem horizontalen Layout organisiert, in dem das Fenster in mehrere Bereiche unterteilt ist.



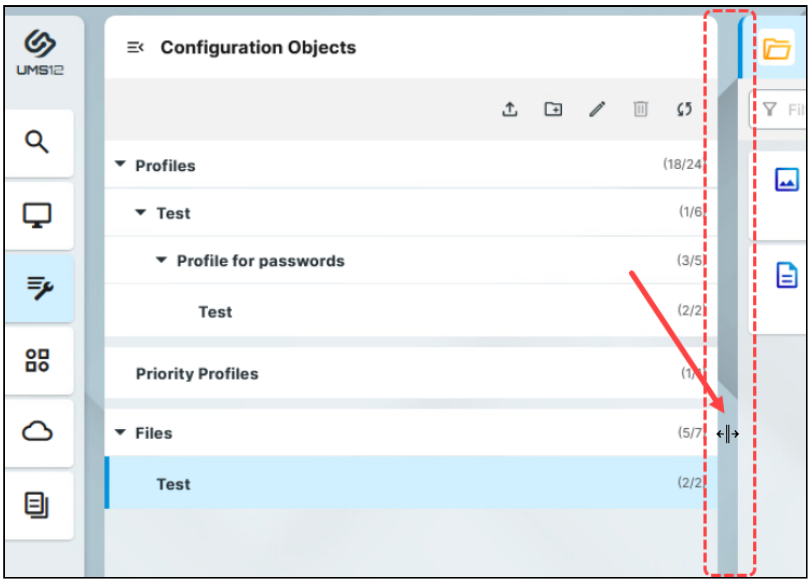
Im Allgemeinen folgen die auf den Tafeln angezeigten Informationen und die Funktionen einer Logik von links nach rechts. Das heißt, Sie finden:

- die Strukturierung auf der linken Seite,
- in der Mitte die Liste der zu verwaltenden Elemente,
- detaillierte Informationen und die Verwaltung der Elemente auf der rechten Seite.

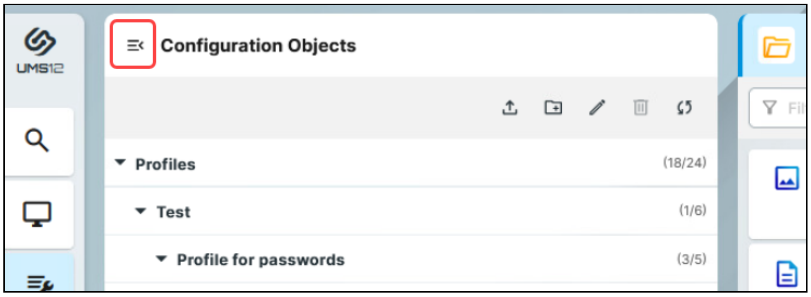
Änderung des Layouts

Sie können die Breite der Tafeln ändern, indem Sie zwischen den Tafeln klicken und gedrückt halten, während Sie die Größe des Feldes ändern:

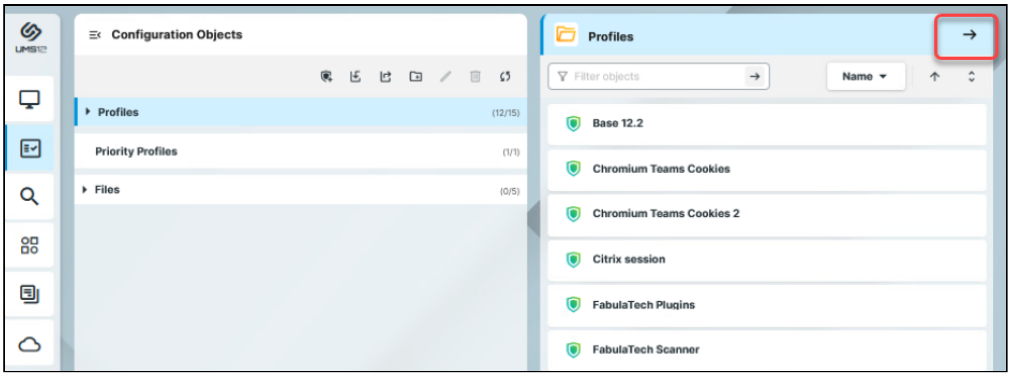
37 http://kb.igel.com

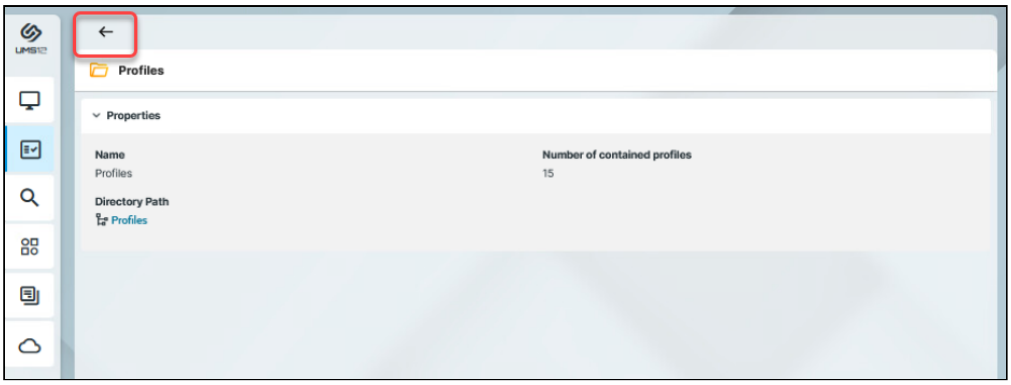


Sie können das linke Fenster ein- und ausklappen, indem Sie auf das Symbol in der oberen Ecke klicken:



Wenn die Größe des Browser-Fensters geändert wird und nicht genügend Platz vorhanden ist, um alle Panels nebeneinander anzuzeigen, können Sie mit Pfeilen zwischen den Panels wechseln:




Profiles
Properties
Name
Profiles
Number of contained profiles
15
Directory Path
Profiles

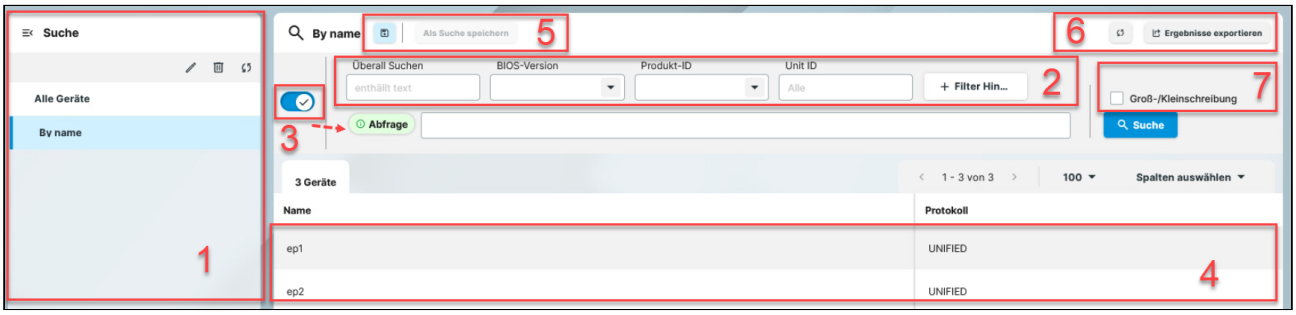
Suche nach Geräten in der IGEL UMS Web App

Im Bereich **Suche** der IGEL Universal Management Suite (UMS) Web App können Sie gemäß den konfigurierten Kriterien nach Geräten suchen.

Sie können auch erweiterte Suchen erstellen, die Sie in Jobs und Verwaltungsaufgaben in der UMS-Konsole verwenden können, siehe Verwendung der erweiterten Suche in Aufgaben und administrative Aufgaben in der UMS Konsole (see page 798).

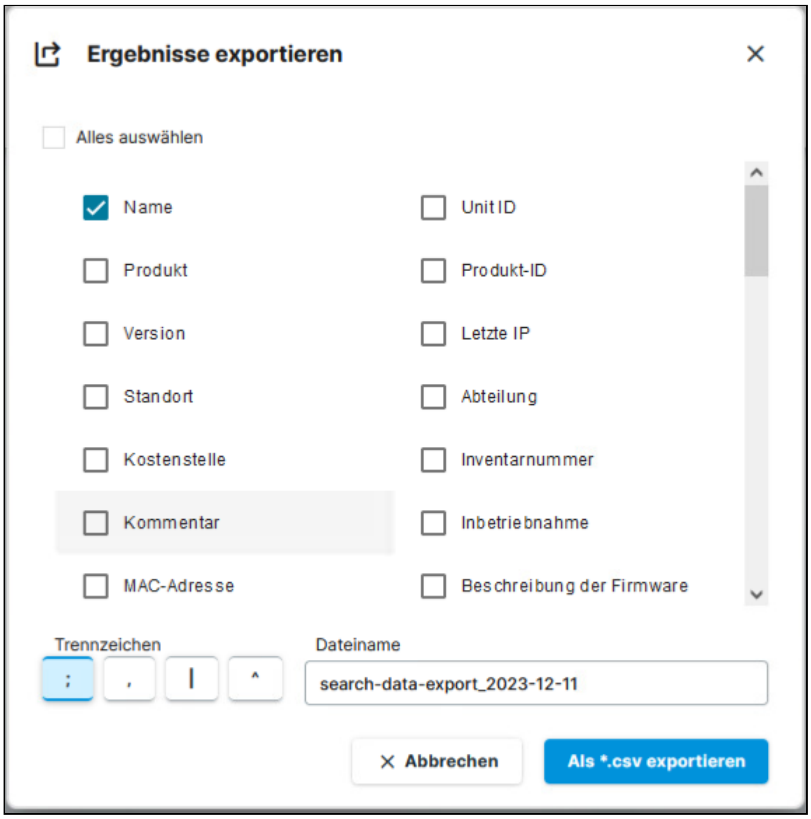
> Die Funktion **Suche** der UMS Web App ist ein Nachfolger der Views in der UMS Konsole (see page 489). Sie bietet derzeit nicht alle Kriterien, die für die Views verfügbar sind, aber der Umfang der Kriterien wird ständig erweitert.

Menüpfad: **UMS Web App > Suche**



1	Liste der Suchen	Zeigt die Liste aller Suchen an, die Sie über die Schaltfläche **Als Suche speichern** gespeichert haben. In der Liste **Alle Geräte** werden alle in der UMS registrierten Geräte angezeigt, für die keine Werte in den Filtern festgelegt wurden. ▶ Um eine Suche umzubenennen, klicken Sie  , geben Sie einen neuen Namen ein und drücken Sie `[Enter]`. ▶ Um eine Suche zu löschen, klicken Sie  . Die Suchen werden dauerhaft entfernt, d.h. ohne Verschiebung in den Papierkorb (see page 545). ▶ Um die Liste zu schließen, klicken Sie  .

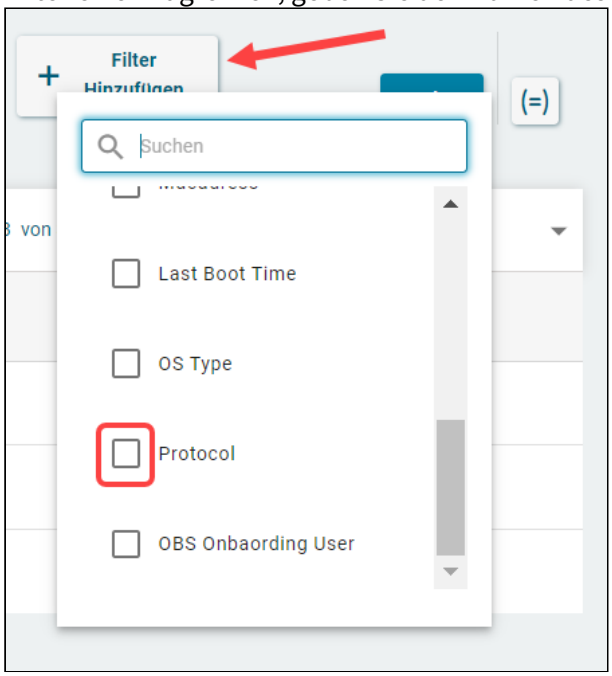
2	Filter	Zeigt alle Filterfelder an, die Sie über die Schaltfläche **Filter Hinzufügen** hinzugefügt haben. ▶ Um ein Filterfeld hinzuzufügen, klicken Sie **Filter Hinzufügen**. Weitere Details finden Sie unter Ein Suchkriterium hinzufügen (see page 796). ⓘ Die Filterauswahl über die Schaltfläche **Filter hinzufügen** ist derzeit begrenzt. Sie können aber mehr Suchkriterien benutzen, wenn Sie auf **Erweiterte Suche (=)** klicken und das Feld **Abfrage** verwenden. ▶ Um ein Filterfeld zu entfernen, klicken Sie 
3	Erweiterte Suche	Die Schaltfläche **Erweitert suchen** fügt das Feld **Abfrage** hinzu, das Sie für komplexe Suchen verwenden können. Die wichtigsten Merkmale der Abfrage: • SQL-ähnliche Abfragesprache • Funktion zur automatischen Vervollständigung • Können kopiert und eingefügt werden Details finden Sie unter Erweiterte Suche für komplexe Abfragen verwenden (see page 797).
4	Suchergebnisse	Listet die Geräte auf, die die angegebenen Suchkriterien erfüllen. Mit einem Klick auf einem Gerätenamen wird ein neuer Tab mit den Informationen zu diesem Gerät geöffnet, siehe Geräte - Ihre Endgeräte in der IGEL UMS Web App ansehen und verwalten (see page 799). Um die Liste zu verwalten, haben Sie folgende Möglichkeiten: • Spalten für die Suchergebnisliste hinzufügen / entfernen • Paging für die Navigation in der Suchergebnisliste • Anzahl der auf einer Seite anzuzeigenden Geräte definieren

5	Als Suche speichern	Wenn Sie auf die Schaltfläche **Als Suche speichern** klicken, wird Ihre aktuelle Suche gespeichert, so dass Sie über die Liste der Suchen darauf zugreifen können. Wenn Sie auf das Symbol **Änderungen schicken** klicken, werden die Änderungen gespeichert, die Sie an der bereits gespeicherten Suche vorgenommen haben.
6	Ergebnisse exportieren	Durch Klicken auf die Schaltfläche **Ergebnisse exportieren** wird der Dialog **Ergebnisse exportieren** geöffnet, in dem die Parameter und Trennzeichen für die CSV-Exportdatei konfiguriert werden können. Spalten, die unter **Spalten auswählen** im Suchergebnisbereich aktiviert wurden, werden automatisch in die Exportdatei aufgenommen, wenn sie nicht manuell im Dialog **Ergebnisse exportieren** deaktiviert werden. 

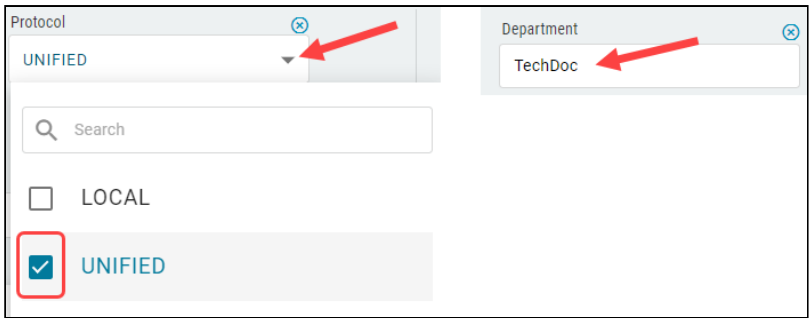
7	Groß/ Kleinschreibung	Wenn die **Groß/ Kleinschreibung** aktiviert ist, wird bei der Eingabe in alle Textfelder die Groß- und Kleinschreibung berücksichtigt. Ist die **Groß/ Kleinschreibung** deaktiviert, wird die Suche ohne Berücksichtigung der Groß- und Kleinstschreibung durchgeführt. Um die Suche nach Groß- und Kleinschreibung nur für ausgewählte Felder einzustellen, fügen Sie das Präfix **cs.** zu den Werten in der WQL-Abfrage hinzu. Zum Beispiel: 

Ein Suchkriterium hinzufügen

1. Klicken Sie **Filter hinzufügen** und wählen Sie das gewünschte Suchkriterium aus. Um die Liste der Kriterien einzugrenzen, geben Sie den Namen des Kriteriums in das Feld **Suchen** ein:



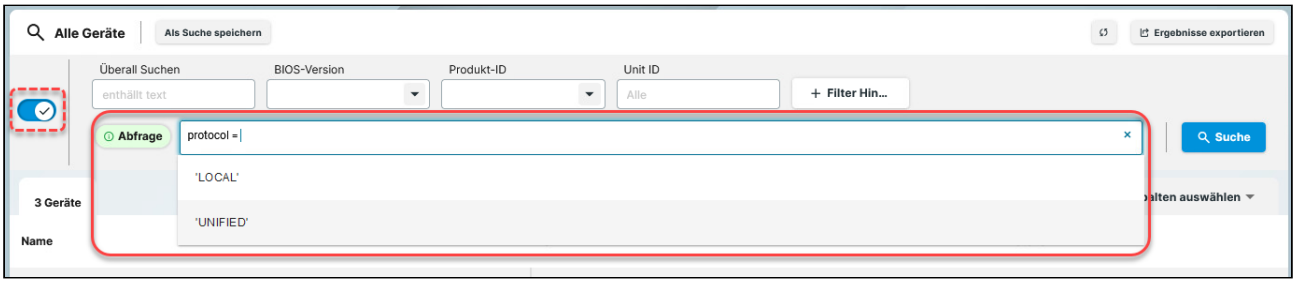
2. Je nach Kriterium wählen Sie den Wert aus der Dropdown-Liste oder geben Sie den Wert in das Feld ein.



Erweiterte Suche für komplexe Abfragen verwenden

Die erweiterte Suche verwendet Autovervollständigung, die auch funktioniert, wenn ein Kriterium/Operator/Wert nur partiell eingegeben wird. Es werden dann nur Treffer angezeigt, die mit dem bereits eingegebenen Fragment übereinstimmen.

So verwenden Sie die erweiterte Suche:



1. Aktivieren Sie die **Abfrage** über die Umschalttaste **Erweitert suchen**.

2. Klicken Sie in das Abfragefeld.
   Die Liste der verfügbaren Kriterien wird angezeigt.

3. Wählen Sie das gewünschte Kriterium aus der Liste aus.
   Je nach ausgewähltem Kriterium wird die Liste der verfügbaren Operatoren angezeigt.

4. Wählen Sie den gewünschten Operator aus.
   Je nach ausgewähltem Operator wird die Liste der verfügbaren Werte angezeigt.

5. Wählen Sie den Wert aus.

6. Um weitere Kriterien zu definieren, wählen Sie einen der logischen Operatoren AND oder OR.

7. Nach Abschluss der Abfrage drücken Sie [Enter] oder klicken Sie **Suchen**.
   Die Liste der Suchergebnisse wird aktualisiert.
   Wenn die Abfrage einen Fehler enthält, wird eine Fehlermeldung angezeigt, die das Problem

erklärt.

8. Sie können die Suche speichern, indem Sie auf **Als Suche speicher**n klicken.

Verwendung der erweiterten Suche in Aufgaben und administrative Aufgaben in der UMS Konsole

In Aufgaben können Sie die gespeicherten erweiterten Suche als Zuweisungsobjekte verwenden. Für weitere Informationen siehe Neue Aufgabe anlegen (see page 519) und Zuordnung (see page 527)

Sie können die gespeicherten Voraussuchen in den folgenden administrative Aufgaben verwenden:

- Geräte löschen (see page 618)
- View oder Advanced Search Ergebnisse via Mail exportieren (see page 621)
- View oder Advanced Search Ergebnisse im Dateisystem speichern (see page 624)
- Objekte zu den Geräten von Views oder Geräte-Suchen zuordnen (see page 627)
- Entferne Objektzuordnungen von Geräten von Views oder Geräte-Suche (see page 630)

⚠
- Die neu gespeicherten Suchen werden nach der Aktualisierung der UMS Konsole angezeigt.
- Durch die Aktualisierung der erweiterten Suche werden die Aufgaben, in denen sie verwendet wird, automatisch aktualisiert.

Geräte - Ihre Endgeräte in der IGEL UMS Web App ansehen und verwalten

Im Bereich **Geräte** der IGEL Universal Management Suite (UMS) Web App können Sie die am UMS Server registrierten Endgeräte verwalten. Alle am UMS Server registrierten Geräte werden angezeigt.

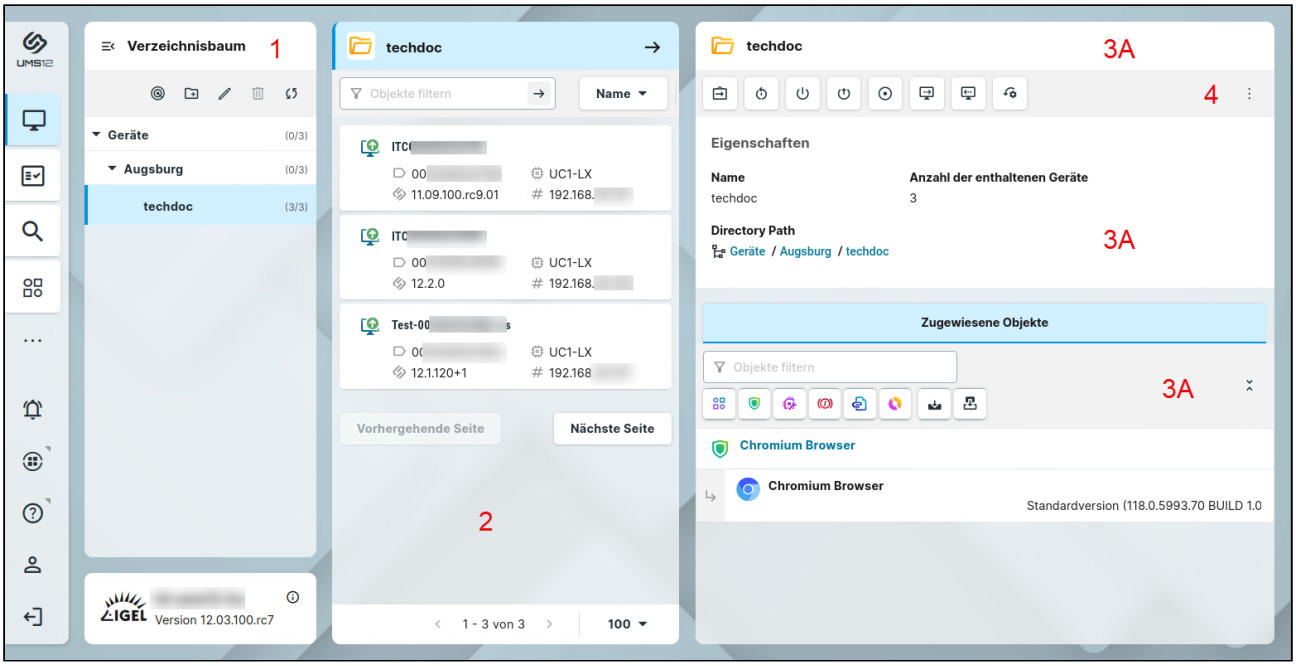
> In der UMS Konsole vorgenommene Änderungen an Geräten sind sofort in der UMS Web App verfügbar, und umgekehrt.

Menüpfad: **UMS Web App > Geräte**

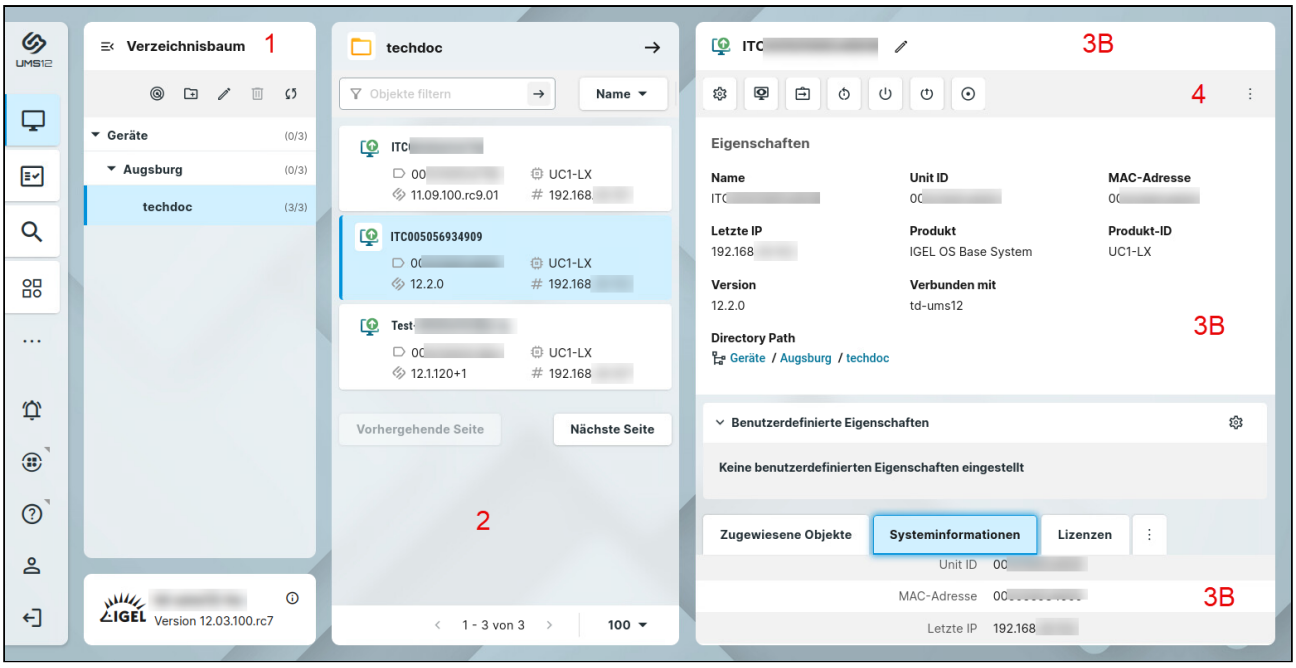
Sie können den Bereich **Geräte** strukturieren, indem Sie Verzeichnisse und gegebenenfalls Unterverzeichnisse anlegen. Dabei ist zu beachten, dass jedes Gerät nur in einem einzigen Verzeichnis abgelegt sein kann.

> Vermeiden Sie es, zu viele Geräte in ein Verzeichnis zu platzieren. Wenn es zu Verzögerungen kommt, beachten Sie die Tipps zur Verzeichnisstruktur unter Leistungsoptimierungen (see page 294).

Verzeichnisebene:



Geräteebene:



1	Verzeichnisbaum	Zeigt alle erstellten Verzeichnisse und Unterverzeichnisse an. Das Format (x/y) gibt 1) die Anzahl der direkt im Verzeichnis enthaltenen Geräte und 2) die Gesamtzahl der Geräte im Verzeichnis und allen Unterverzeichnissen dieses Verzeichnisses an. • Verzeichnisstruktur in der IGEL UMS Web App erstellen (see page 809) • Verzeichnis in der IGEL UMS Web App umbenennen (see page 813) • Verzeichnis in der IGEL UMS Web App löschen (see page 814) • Geräteverzeichnis verschieben (see page 812) • Geräteverzeichnis in der IGEL UMS Web App kopieren (see page 811) • Geräte in der IGEL UMS Web App verschieben (see page 810) • Netzwerk nach Geräten scannen und Geräte an der IGEL UMS registrieren (see page 324)
2	Geräteliste	Zeigt alle Geräte an, die direkt in dem im **Verzeichnisbaum** ausgewählten Verzeichnis enthalten sind. • Paging für die Navigation in der Geräteliste • Anzahl der auf einer Seite anzuzeigenden Geräte definieren • Geräte nach **Name**, **Produkt-ID**, **Unit ID**, **Version** und **IP-Adresse** filtern • Geräte nach **Name**, **Produkt-ID**, **Unit ID**, **Version** und **IP-Adresse** sortieren • Ein Rechtsklick auf das Gerät öffnet das Kontextmenü.

3A	Verzeichnisinformationen	Details für das im **Verzeichnisbaum** markierte Verzeichnis **[Verzeichnisname]**: Name des markierten Verzeichnisses **Eigenschaften**: Eigenschaften des markierten Verzeichnisses, z.B. der vollständige **Verzeichnispfad** oder die **Anzahl der enthaltenen Geräte** **Zugewiesene Objekte**: Direkt und indirekt zugeordnete Objekte, z.B. Profile, Dateien, Firmwareupdates usw. Für Details siehe Objekte in der IGEL UMS Web App zuweisen (see page 815).

3B	Geräteinformationen	Details für das in der Geräteliste markierte Gerät **Statusanzeige** Status des markierten Geräts. Symbole, die den Gerätestatus anzeigen, finden Sie unten unter "Statusanzeigen (see page 805)". **[Gerätename]** Name des markierten Geräts. Er muss nicht mit dem Namen des Geräts im Netzwerk identisch sein. Der Name eines Geräts muss nicht eindeutig sein und kann mehrfach verwendet werden. Um das Gerät umzubenennen, klicken Sie auf  , geben Sie einen neuen Namen ein, und drücken Sie [Enter]. Weitere Optionen für die Umbenennung finden Sie unter Renaming IGEL OS Devices (see page 799). **Eigenschaften** Eigenschaften des markierten Geräts, z.B. **Letzte IP**, **MAC-Adresse**, **Unit ID**, Letzter Kontakt (see page 799) usw. ⓘ Die Unit ID dient als eindeutiges Identifizierungsmerkmal eines Endgeräts in der UMS. Bei IGEL Geräten, IGEL Zero Clients, Geräten, die mit IGEL UDC/OSC konvertiert wurden, sowie Geräten mit IGEL UMA wird die Unit ID mit der MAC-Adresse des Geräts belegt. Wenn das Gerät ein UD Pocket ist, so wird die Unit ID mit der Seriennummer (ohne Leerzeichen und Sonderzeichen) belegt, der ein Präfix vorangestellt ist, das aus der USB-Hersteller- und Produkt-ID besteht. **[Verzeichnispfad]** Der vollständige Verzeichnispfad für das ausgewählte Gerät **Benutzerdefinierte Eigenschaften** Ermöglicht die Änderung solcher benutzerdefinierbaren Eigenschaften wie **Website**, **Abteilung**, Geräteattribute. Um die Eigenschaften zu bearbeiten, klicken Sie auf  .

Benutzerdefinierte Geräteattribute
Geräteattribute sind derzeit nur in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Geräteattribute** konfigurierbar.
Ob Sie die Werte für die Geräteattribute über die UMS Web App ändern können, hängt von Ihrer Konfiguration für die **Globale Überschreiberegel** und/oder die **Überschreiberegel** für ein bestimmtes Geräteattribut ab, siehe Geräteattribute für IGEL OS Geräte verwalten (see page 593).

Die folgenden Bereiche werden nur angezeigt, wenn für den Bereich Daten verfügbar sind:

- **Lizenzen**
- **Netzwerkadapter**
- **Installierte Apps**

- **Historie erfolgreicher Benutzeranmeldungen**

Zugewiesene Objekte
Zeigt direkt und indirekt zugeordnete Objekte, z.B. Profile, Apps, Dateien, usw. Für Details siehe Objekte in der IGEL UMS Web App zuweisen (see page 815).

Systeminformationen
Zeigt solche Eigenschaften wie **CPU-Typ**, **Arbeitsspeicher**, **Gerätetyp** usw. an. Um den Wert zu kopieren, klicken Sie auf  .

Lizenzen
Details zu den Lizenzen für das ausgewählte Gerät. Um einen Wert zu kopieren, klicken Sie auf  .

Netzwerkadapter
Zeigt Informationen über alle verfügbaren Netzwerkadapter eines Geräts an. Der Bereich ist für Geräte mit IGEL OS 11.07.100 oder höher verfügbar. Für Details, siehe Abschnitt "Netzwerkadapter" unter Geräteinformationen in der IGEL UMS einsehen (see page 449).

Installierte Apps
Zeigt alle auf dem IGEL OS 12-Gerät vorhandenen Apps, deren Status und den Zeitpunkt an, wenn das Gerät die Meldung über den App-Status übermittelt hat. Für Details, siehe Checking Installed Apps via the IGEL UMS Web App (see page 882).

Historie erfolgreicher Benutzeranmeldungen
Zeigt bis zu 10 letzte Benutzeranmeldungen an, wenn die Protokollierung aktiviert ist. Einzelheiten zur Aktivierung der Protokollierung finden Sie im Abschnitt "Historie erfolgreicher Benutzeranmeldungen" unter Geräteinformationen in der IGEL UMS einsehen (see page 449).

4	Gerätebefehle	Gerätebefehle, z.B. Befehle für Energiesteuerung, Firmwareupdate, usw., werden für ein einzelnes Verzeichnis oder für ein einzelnes Gerät ausgeführt. Der Status der Befehlsausführung wird unter Nachrichten (see page 787) angezeigt. ▶ Klicken Sie, um alle verfügbaren Gerätebefehle anzuzeigen. Details zu den Gerätebefehlen finden Sie unter "Gerätebefehle (see page 806)" unten.

Statusanzeigen

Die UMS überwacht den Status der Geräte durch regelmäßiges Senden von UDP-Paketen. Gemäß Voreinstellung geschieht dies alle 3 Sekunden. Wie Sie das Abfrageintervall für die Onlineprüfung ändern können, finden Sie unter Geräte (see page 447).

Wenn das Gerät über den IGEL Cloud Gateway (ICG) verbunden ist, erhält das Gerät ein Wolkensymbol .

Das Ausrufezeichen weist darauf hin, dass Änderungen, d.h. neue Konfigurationen, Profile, Dateien usw., noch nicht zum Gerät übertragen wurden.

Symbole für IGEL OS Geräte

Die folgenden Symbole zeigen den Status eines IGEL OS Geräts an:

	Das Gerät ist online.
	Das Gerät ist offline.
	Das Gerät wird gerade aktualisiert.
	Der Gerätestatus ist unbekannt oder wurde noch nicht geladen.

Gerätebefehle

Die folgenden Befehle können sowohl für ein einzelnes Gerät als auch für ein einzelnes Verzeichnis (außer Spiegeln und Bearbeitung der Konfiguration) ausgeführt werden.

Konfiguration bearbeiten	Konfigurationsparameter des ausgewählten Geräts bearbeiten. Hier bearbeiten Sie die Geräteeinstellungen so, als ob Sie am Endgerät selbst arbeiten würden.
Spiegeln	Spiegeln: Startet eine VNC-Sitzung für das markierte Gerät, falls Spiegeln für dieses Gerät aktiviert ist, siehe Spiegeln. Für Details zum Spiegeln in der UMS siehe Spiegeln - IGEL OS Desktop über VNC beobachten (see page 481) und UMS und Geräte: Sicheres Spiegeln (see page 39).
Objekt zuweisen	Weist dem markierten Gerät ein Objekt, z.B. ein Profil oder eine Datei, zu oder entfernt die Zuordnung. Für Details siehe Objekte in der IGEL UMS Web App zuweisen (see page 815).
Systemneustart	Führt bei dem markierten Gerät einen Neustart durch.
Herunterfahren	Fährt das markierte Gerät herunter.
Hochfahren	Startet das markierte Gerät über das Netzwerk (Wake-on-LAN). Einzelheiten zur Konfiguration von Wake-on-LAN in der UMS finden Sie unter Wake-on-LAN (see page 654).
Standbymodus	Setzt das markierte Gerät in den Standbymodus.
Einstellungen senden	Liest die komplette letzte Gerätekonfiguration aus der UMS Datenbank aus und sendet sie an das markierte Gerät.
Einstellungen erhalten	Liest die lokale Konfiguration des markierten Geräts, sendet sie an die UMS und schreibt sie in die Datenbank.

Auf Werkseinstellungen zurücksetzen	Setzt das markierte Gerät auf die Werkseinstellungen zurück; siehe Zurücksetzen eines Geräts auf die Werkseinstellungen über die IGEL UMS Web App (see page 822). Weitere Methoden zum Zurücksetzen eines Geräts auf die Werkseinstellungen finden Sie unter Reset to Factory Defaults und Zurücksetzen eines Geräts mit unbekanntem Administratorpasswort.
Update	OS 11: Führt bei dem markierten IGEL OS 11-Gerät ein Firmwareupdate aus. OS 12: Löst die Aktivierung der zugewiesenen App-Version bei den markierten IGEL OS 12-Geräten aus. Der **Update**-Befehl wird nur benötigt, wenn **System > Update > App nach der Installation aktivieren** deaktiviert ist; siehe How to Configure the Background App Update in the IGEL UMS Web App (see page 893).
Update beim Herunterfahren	Nur für OS 11: Führt ein Firmwareupdate aus, wenn das markierte IGEL OS 11-Gerät heruntergefahren wird.
Systeminformationen aktualisieren	Aktualisiert die Systeminformationen für das markierte Gerät.
Lizenzinformationen aktualisieren	Aktualisiert die Lizenzinformationen für das markierte Gerät.
Als Profil exportieren	Exportiert Geräteeinstellungen, siehe Geräteeinstellungen als Profil in der IGEL UMS Web App exportieren (see page 826).
Nachricht senden	Sendet eine Nachricht an das markierte Gerät; siehe Eine Nachricht an Geräte über die IGEL UMS Web App senden (see page 820).

Spezifische Befehle	Öffnet ein Menü der gerätespezifischen Befehle, die für das Verzeichnis oder das Gerät verfügbar sind. Welche Befehle verfügbar sind, hängt von den folgenden Kriterien ab: • Das Gerät hat IGEL OS 12.3 oder höher. • Eine App, die spezifische Befehle unterstützt, ist auf dem Gerät installiert.

Wenn ein Benutzer keine ausreichenden Rechte hat, sind die Befehlssymbole ausgegraut. Informationen zu Berechtigungen in der UMS finden Sie unter Zugriffsrechte (see page 678).

Verzeichnisstruktur in der IGEL UMS Web App erstellen

In der IGEL Universal Management Suite (UMS) Web App können Sie Geräteverzeichnisse anlegen. Sie können beliebig viele Verzeichnisse und Unterverzeichnisse erstellen, um die Geräte in Gruppen zusammenzufassen.

Menüpfad: **UMS Web App > Geräte**

Allgemeine Informationen

Ihre Gerätestruktur können Sie in der IGEL UMS frei organisieren. Nutzen Sie diese Freiheit und bauen Sie durchdachte, intelligente Verzeichnisstrukturen auf. Sie benötigen eine intelligente Struktur z.B. für den automatischen Rollout, bei dem die Geräte direkt im richtigen Verzeichnis abgelegt werden und ihnen automatisch die richtigen Konfigurationen (Profile, Apps) zugewiesen werden.

Wie tief Sie Ihren Baum strukturieren wollen, bestimmen Sie selbst. Das System ermöglicht es Ihnen, Verzeichnisse so tief zu verschachteln, wie Sie es wünschen.

Es ist ratsam, die Verzeichnisse auf die Struktur Ihres Unternehmens abzustimmen. Sie können die Geräte z. B. nach Niederlassungen, Abteilungen oder Aufgaben klassifizieren.

Wenn Sie Unterverzeichnisse erstellen, bilden die darin organisierten Geräte Untergruppen einer Gruppe.

> ⓘ Ein Gerät, das durch seine MAC-Adresse eindeutig identifiziert ist, kann nur in einem einzigen Verzeichnis abgelegt sein, also nur Mitglied einer einzigen Gruppe sein.

> ⓘ Aktionen, die auf der Verzeichnisebene durchgeführt werden, gelten für alle Unterverzeichnisse und Geräte, die in diesem Verzeichnis enthalten sind.
> Für die Durchführung von Aktionen auf Verzeichnisebene sind bestimmte Berechtigungen erforderlich, siehe den Abschnitt "Berechtigungen" unter Wichtige Informationen zur IGEL UMS Web App (see page 784).

Geräteverzeichnis erstellen

So erstellen Sie ein Verzeichnis oder Unterverzeichnis:

1. Wählen Sie im **Verzeichnisbaum** ein Verzeichnis aus, z. B. "Geräte".
2. Klicken Sie  .
3. Geben Sie den Namen für das neue Verzeichnis ein.
4. Drücken Sie [Enter].
   Das neue Verzeichnis wird im **Verzeichnisbaum** unter dem ausgewählten Verzeichnis angezeigt.

Nun können Sie Geräte in dieses neue Verzeichnis verschieben.

Geräte in der IGEL UMS Web App verschieben

Da ein Gerät nur in einem einzigen Verzeichnis in der IGEL Universal Management Suite (UMS) abgelegt sein kann, können Sie Geräte nicht kopieren, sondern nur verschieben.

> ⚠ Werden dem Gerät durch die Neuzuordnung zu einem Verzeichnis indirekt Profile und Apps zugewiesen oder entzogen, so ändert sich die Konfiguration des Geräts. Das Verschieben eines IGEL OS 12-Geräts in ein anderes Verzeichnis kann zur Deinstallation von Apps führen.
> Die neue Konfiguration wird entweder sofort oder beim nächsten Neustart wirksam.

Menüpfad: **UMS Web App > Geräte**

Geräte werden per Drag & Drop verschoben:

1. Wählen Sie im **Verzeichnisbaum** ein Verzeichnis aus, das das zu verschiebende Gerät enthält.
2. Wählen Sie das entsprechende Gerät aus.
3. Ziehen Sie das Gerät in das gewünschte Verzeichnis und legen Sie es dort ab.
   Der Dialog **Gerät verschieben** öffnet sich.
4. Wählen Sie aus, wann die Änderungen wirksam werden sollen.
5. Klicken Sie auf **Verschieben**, um die Verschiebung zu bestätigen.

Geräteverzeichnis in der IGEL UMS Web App kopieren

Sie können ein Geräteverzeichnis kopieren und in ein beliebiges Verzeichnis einfügen. Dabei werden nur das leere Verzeichnis sowie die darin enthaltenen Unterverzeichnisse kopiert; Geräte können nicht kopiert werden.

So kopieren Sie ein Geräteverzeichnis:

1. Klicken Sie im **Verzeichnisbaum** auf das Verzeichnis, das Sie kopieren wollen.
2. Drücken Sie [Strg + C].
3. Klicken Sie das Verzeichnis, in das Sie die Kopie des Verzeichnisses einfügen wollen.
4. Drücken Sie [Strg+ V].
5. Bestätigen Sie den Dialog **Verzeichnis kopieren**.
   Ein neues Geräteverzeichnis wird angelegt, das den gleichen Namen hat wie das ursprüngliche Verzeichnis. Das neue Verzeichnis enthält neu angelegte Kopien der im ursprünglichen Verzeichnis enthaltenen Unterverzeichnisse.

> ⓘ Sie können ein Geräteverzeichnis auch per Drag & Drop kopieren, während Sie die [Strg]-Taste gedrückt halten.

Geräteverzeichnis verschieben

Wenn ein Geräteverzeichnis in ein anderes Verzeichnis verschoben wird, werden das Verzeichnis selbst, seine Unterverzeichnisse und die darin enthaltenen Geräte verschoben.

Menüpfad: **UMS Web App > Geräte**

So verschieben Sie ein Geräteverzeichnis:

1. Im **Verzeichnisbaum** klicken Sie auf das Verzeichnis, das Sie verschieben wollen.
2. Drücken Sie [Strg + X].
3. Klicken Sie auf das Verzeichnis, in das Sie das Verzeichnis verschieben möchten.
4. Drücken Sie [Strg + V].
   Der Dialog **Verzeichnis verschieben** öffnet sich.

   ⚠ Werden dem Gerät durch die Neuzuordnung zu einem Verzeichnis indirekt Profile und Apps zugewiesen oder entzogen, so ändert sich die Konfiguration des Geräts. Das Verschieben eines IGEL OS 12-Geräts in ein anderes Verzeichnis kann zur Deinstallation von Apps führen.
   Die neue Konfiguration wird entweder sofort oder beim nächsten Neustart wirksam.
5. Wählen Sie aus, wann die Änderungen wirksam werden sollen und bestätigen Sie die Auswahl, indem Sie auf **Verschieben** klicken.

ⓘ Sie können ein Verzeichnis auch per Drag & Drop verschieben.

Verzeichnis in der IGEL UMS Web App umbenennen

So benennen Sie ein Verzeichnis oder Unterverzeichnis in der IGEL Universal Management Suite (UMS) Web App um:

1. Gehen Sie zum **Verzeichnisbaum**.
2. Wählen Sie ein Verzeichnis, das Sie umbenennen möchten.
3. Klicken Sie  .
4. Geben Sie einen neuen Namen für das Verzeichnis ein.
5. Drücken Sie [Enter].

Verzeichnis in der IGEL UMS Web App löschen

Die Löschung eines Verzeichnisses in der IGEL Universal Management Suite (UMS) Web App ist nur möglich, wenn das Verzeichnis keine Geräte enthält.

> Derzeit wird der Papierkorb NICHT unterstützt. Wenn Sie ein Verzeichnis löschen, wird es dauerhaft entfernt.

So löschen Sie ein Verzeichnis:

1. Im **Verzeichnisbaum** wählen Sie das zu löschende Verzeichnis aus.
2. Klicken Sie  .

   > Wird ein Verzeichnis gelöscht, so werden auch alle darin enthaltenen Unterverzeichnisse gelöscht.
3. Bestätigen Sie den Dialog **Verzeichnis löschen**.

Objekte in der IGEL UMS Web App zuweisen

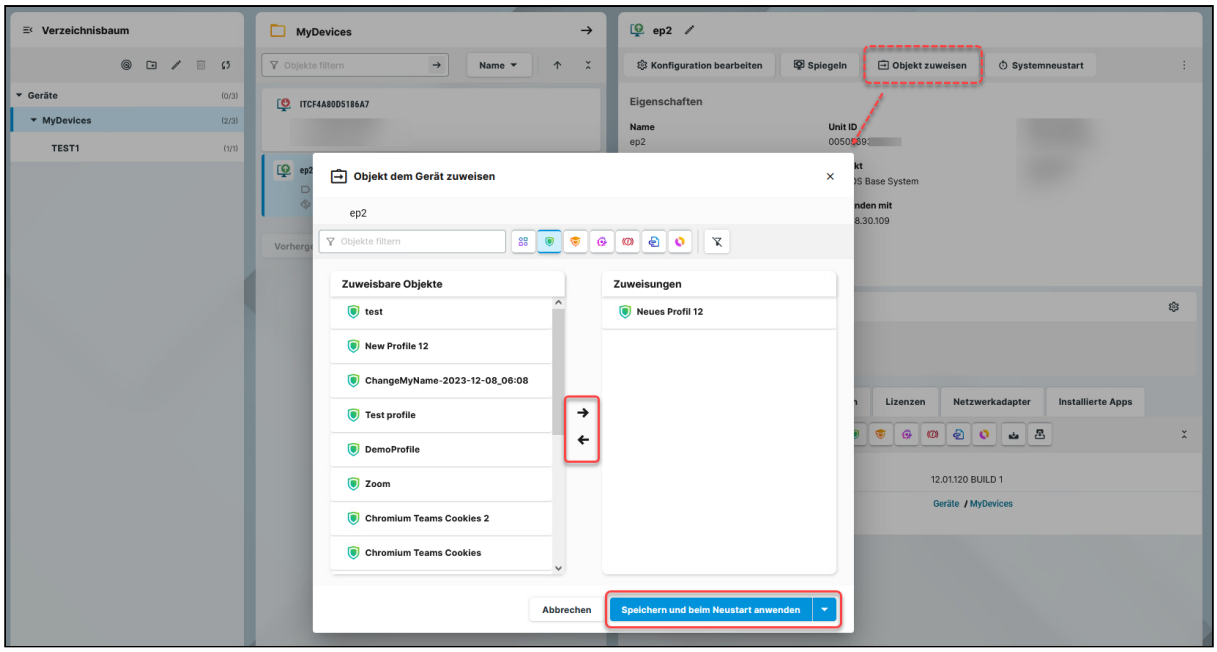
In der IGEL Universal Management Suite (UMS) Web App können Sie einem Gerät oder Geräteverzeichnis ein Objekt (z.B. Datei, Profil, App, usw.) zuweisen.

Menüpfad: **UMS Web App > Geräte**

Um ein Objekt zuzuweisen (oder zu entfernen), gehen Sie wie folgt vor:

1. Wählen Sie unter **UMS Web App > Geräte** das gewünschte Verzeichnis / Gerät aus und klicken Sie **Objekt zuweisen**.

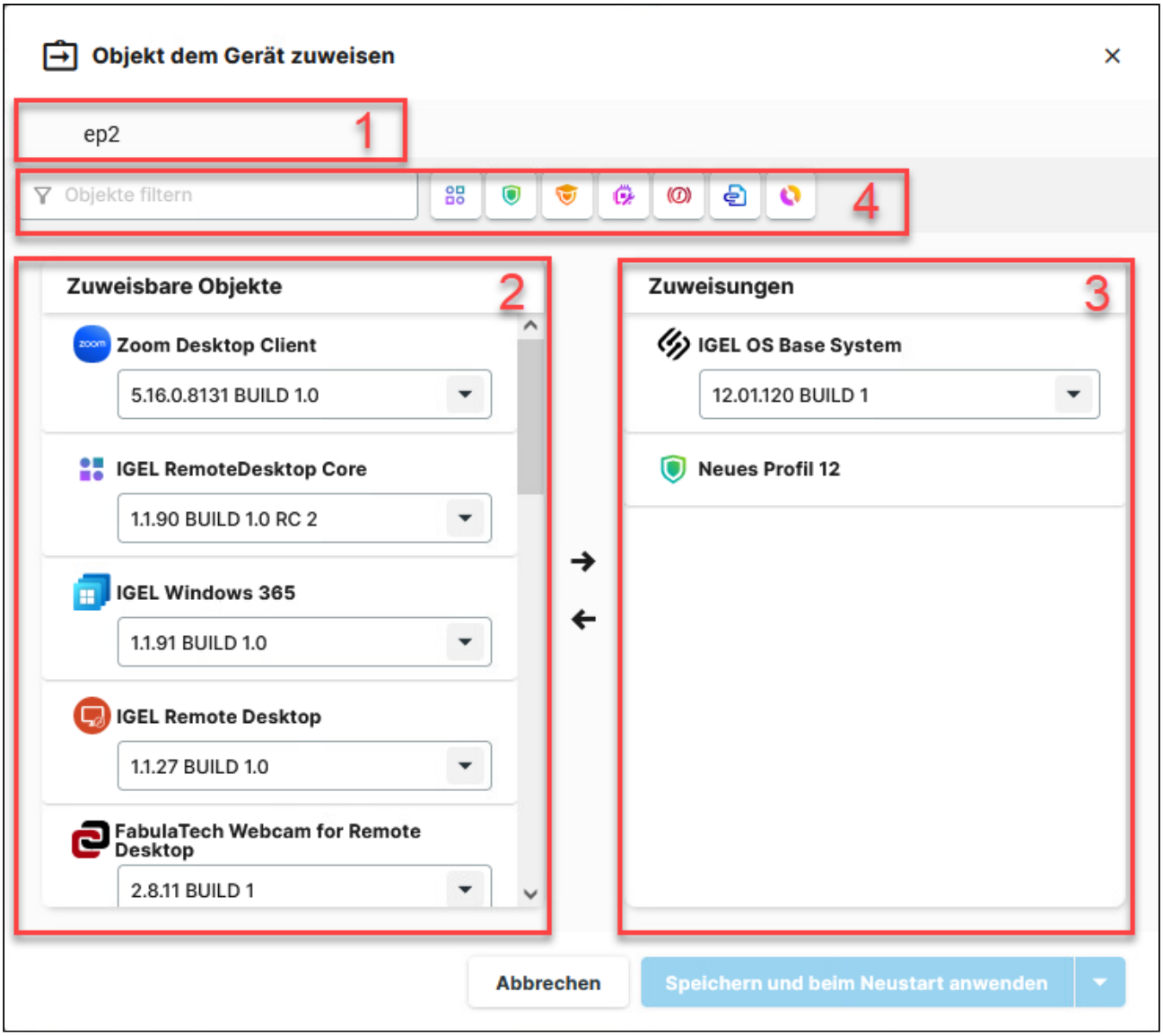
   Es ist nicht möglich, ein Objekt dem Stammverzeichnis "Geräte" zuzuweisen.



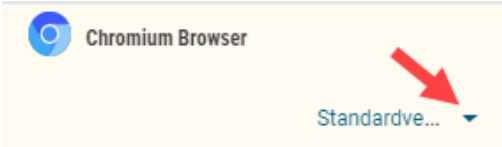
2. Wählen Sie das gewünschte Objekt aus und verwenden Sie die Pfeilschaltflächen oder Drag & Drop.

3. Entscheiden Sie, ob die neuen Einstellungen sofort oder beim nächsten Start des Geräts wirksam werden sollen.

Objekt dem Gerät zuweisen Dialog



1	Name des Verzeichnisses / Geräts	Name des Verzeichnisses / Geräts, dem das Objekt zugeordnet ist
2	Zuweisbare Objekte	Zeigt alle Objekte an, die dem Verzeichnis / Gerät zugewiesen werden können. Die folgenden Objekte können zugeordnet werden:

		: Apps (für IGEL OS 12-Geräte). Eine zuzuweisende App-Version wird in der Auswahlliste selektiert, die alle unter Apps (see page 862) verfügbaren Versionen der markierten App anzeigt.  **Implizite App-Zuweisung über ein Profil** Eine App wird automatisch über ein Profil zugewiesen, das diese App konfiguriert. Ausnahmen: IGEL OS Base System App Eine implizite App-Zuweisung wird überschrieben, wenn Sie eine App explizit zuweisen, d. h. wenn Sie eine App als Objekt im Dialog **Objekt zuweisen** auswählen. Weitere Informationen finden Sie unter Profile in der IGEL UMS Web App erstellen und zuweisen (see page 838).
		: Profile. Für allgemeine Informationen zu Profilen, siehe Profile in der IGEL UMS (see page 365). Siehe auch Konfiguration - Zentralisierte Verwaltung von Geräteeinstellungen in der IGEL UMS Web App (see page 828).
		: Priority Profile. Für Details siehe Priority Profile in der IGEL UMS (see page 413).
		: Firmwareanpassungen. Für Details siehe Firmwareanpassungen in der IGEL UMS (see page 435).
		: Templateschlüssel und Wertesammlungen. Für Details siehe Templateprofile in der IGEL UMS (see page 416).
		: Dateien. Für Details siehe Dateien - Dateien am IGEL UMS Server registrieren und zu Geräten übertragen (see page 529).
		: Firmwareupdates (für IGEL OS 11-Geräte). Für Details siehe Universal Firmware Update (see page 539).
3	Zuweisungen	Zeigt alle Objekte an, die direkt dem Verzeichnis / Gerät zugeordnet sind.

4	Filter	Filtert die Objekte unter **Zuweisbare Objekte** und **Zuweisungen** nach • ausgewähltem Objekttyp • Eingabe im Textfeld Die obigen Filterkriterien werden mit dem Operator *AND* verknüpft. ▶ Klicken Sie , um alle Filter zu entfernen.

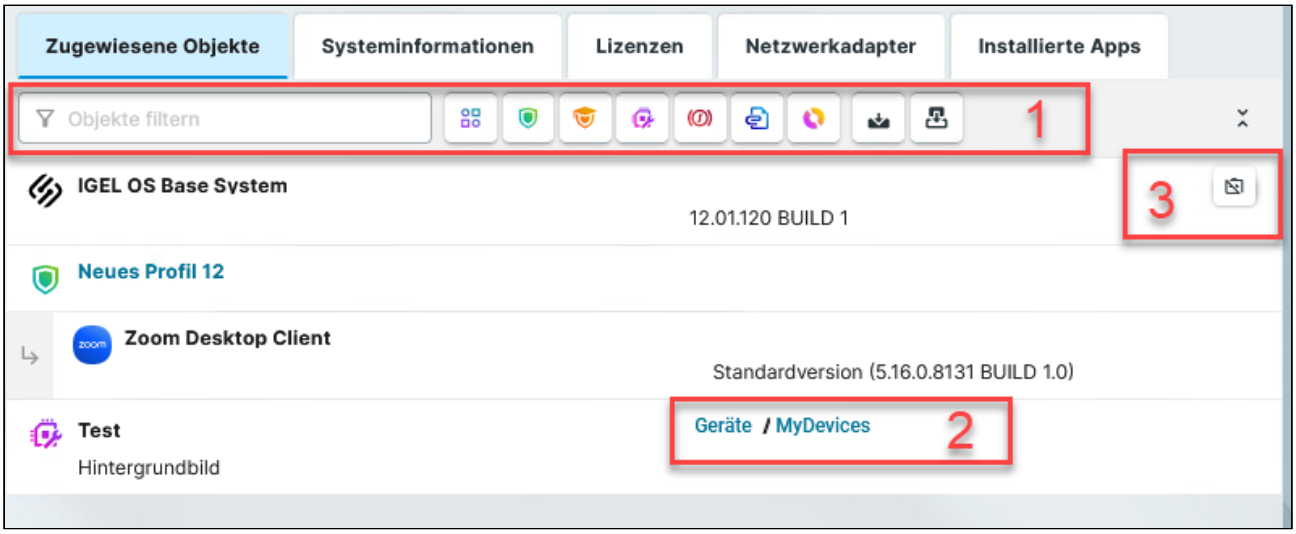
Zugewiesene Objekte

Objekte können direkt oder indirekt zugeordnet werden:

- Direkt zugeordnete Objekte wurden einem einzelnen Gerät oder Ordner zugewiesen.
- Indirekt zugeordnete Objekte wurden über die Ordnerstruktur 'geerbt'.

▶ Um alle zugewiesenen Objekte anzuzeigen, d.h. direkt und indirekt zugewiesene Objekte, wählen Sie das gewünschte Verzeichnis / Gerät aus und gehen Sie zu **Zugewiesene Objekte**.

> ⓘ Alle implizit zugewiesenen Apps, d. h. Apps, die Geräten über ein Profil zugewiesen sind, werden direkt unter diesem Profil angezeigt.



1	Filtert zugeordnete Objekte nach • ausgewähltem Objekttyp • Eingabe im Textfeld • direktem oder indirektem Zuweisungstyp Die obigen Filterkriterien werden mit dem Operator *AND* verknüpft. ▶ Klicken Sie  , um alle Filter zu entfernen.
2	Nur für indirekt zugeordnete Objekte: Gibt den Pfad zu dem Verzeichnis an, von dem die Objektzuordnung geerbt wird.
3	Nur für direkt zugeordnete Objekte: Entfernt das Objekt von dem Verzeichnis / Gerät.

Eine Nachricht an Geräte über die IGEL UMS Web App senden

In der IGEL Universal Management Suite (UMS) Web App können Sie eine Nachricht an IGEL OS 12-Geräte senden. Derzeit werden nur Nachrichten im Klartext unterstützt, d.h. Nachrichten in Form von einfachen Strings ohne Formatierung und HTML-Codes.

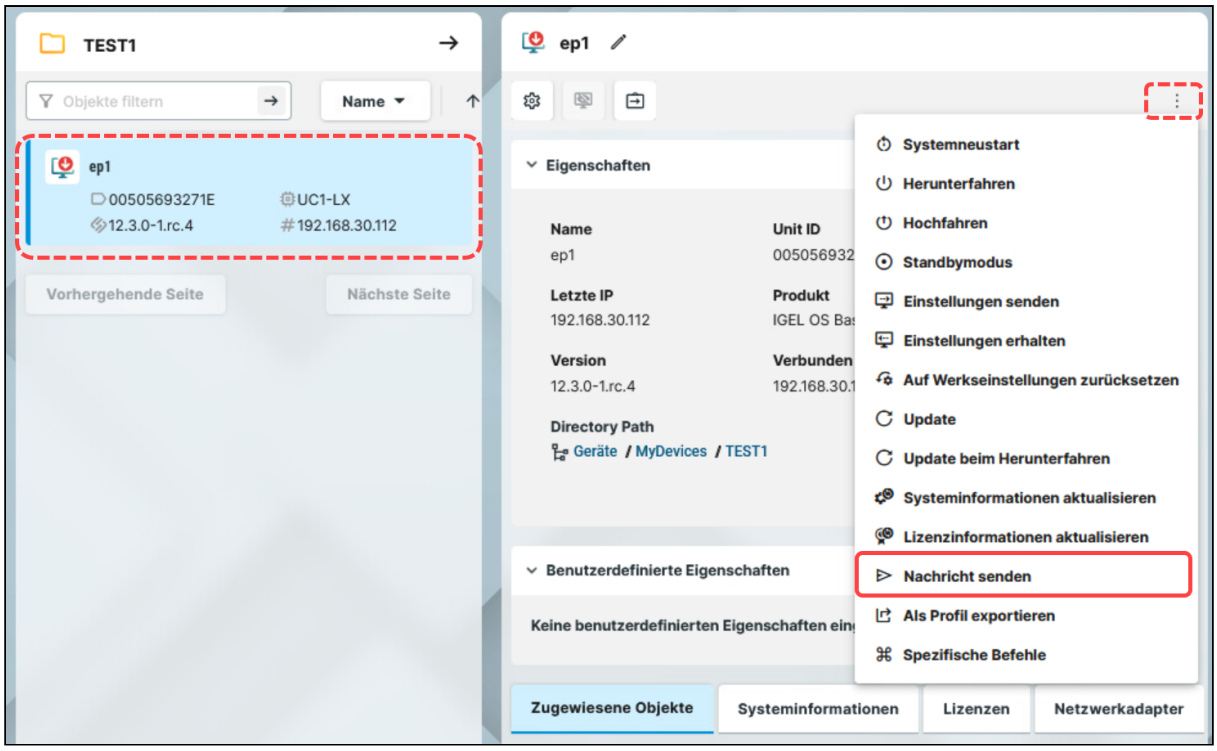
Das Senden einer Nachricht an IGEL OS 11-Geräte über die UMS Web App ist derzeit nicht möglich. Verwenden Sie stattdessen die UMS Konsole; siehe Nachricht senden (see page 474).

Menüpfad: **UMS Web App > Geräte > Nachricht senden**

> Um eine Nachricht an IGEL OS 12-Geräte zu senden, sind die folgenden Berechtigungen erforderlich:
> - **Lesen** und **Nachricht senden** (gesetzt unter **UMS Konsole > [Kontextmenü eines Geräts / Geräteverzeichnisses] > Berechtigungen**)
> - **Massenhafte Geräte-Aktionen**, wenn eine Nachricht an mehrere Geräte gesendet werden soll (gesetzt unter **UMS Konsole > System > Administratorkonten**)
>
> Allgemeine Informationen zu Berechtigungen finden Sie unter Administratorkonten und Zugriffsrechte (see page 676).

So senden Sie eine Nachricht:

1. Wählen Sie in der **UMS Web App > Geräte** das gewünschte Gerät / Geräteverzeichnis aus und klicken Sie **Nachricht senden**.

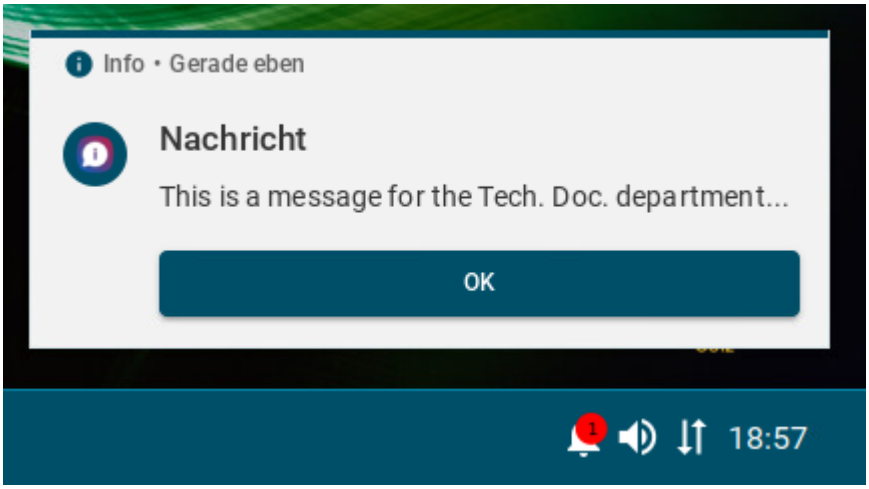


2. Schreiben Sie Ihre Nachricht. Verwenden Sie keine HTML- oder anderen Codes.

3. Klicken Sie **Nachricht senden**.

Ihre Nachricht wird an die in der Liste aufgeführten Geräte gesendet. Diese Geräteliste ist nur zum Lesen gedacht, d.h. Sie können die Geräte hier nicht auswählen.
Wenn Sie das Geräteverzeichnis für den Nachrichtenversand ausgewählt haben, wird die Anzahl der betroffenen Geräte angezeigt.

Auf dem Gerät wird die Nachricht in einem Nachrichtenfenster und, falls nicht geschlossen, auch im Benachrichtigungscenter angezeigt.



Zurücksetzen eines Geräts auf die Werkseinstellungen über die IGEL UMS Web App

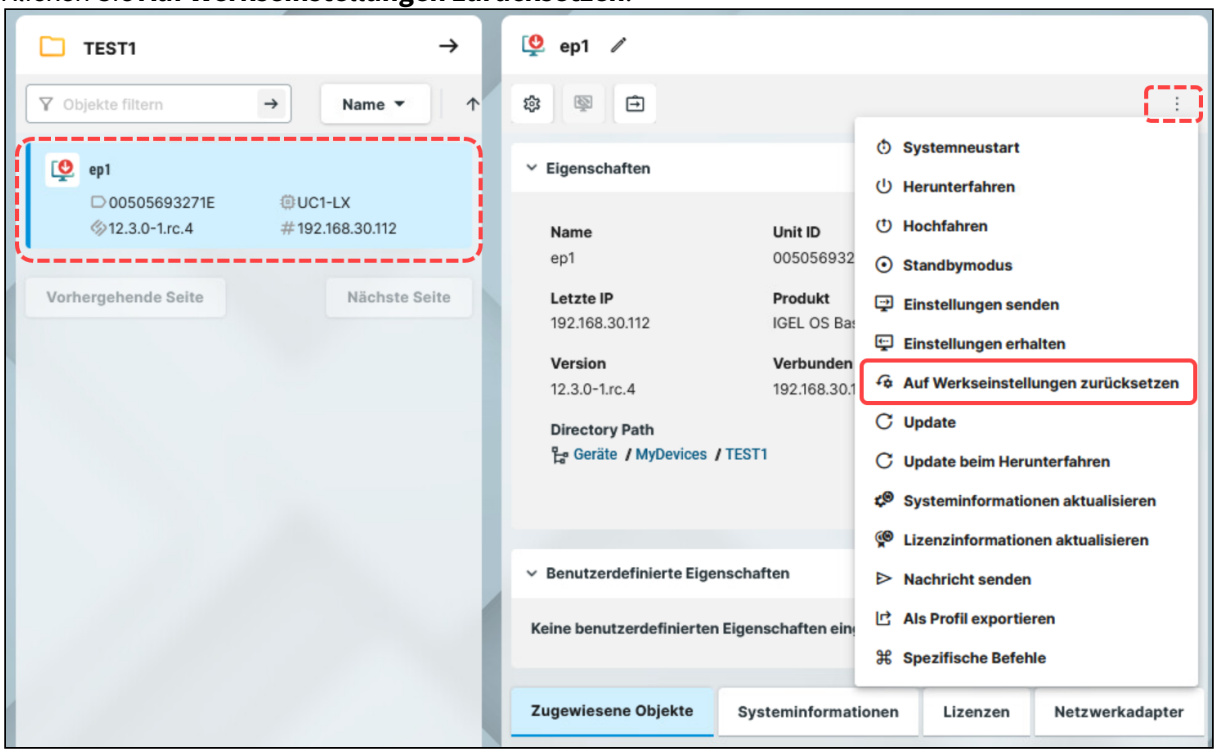
In der IGEL Universal Management Suite (UMS) Web App können Sie ein Gerät auf die Werkseinstellungen zurücksetzen. Dies kann z. B. aufgrund einer Fehlkonfiguration notwendig sein oder wenn das Administratorpasswort für IGEL OS verloren gegangen ist und somit das lokale Setup nicht mehr zugänglich ist.

> ⚠ Beim **Zurücksetzen auf Werkseinstellungen** (Reset to Factory Defaults) gehen alle persönlichen Einstellungen auf dem Gerät verloren, darunter auch Ihr Passwort und Ihre konfigurierten Sitzungen. Das Gerät wird aus der UMS entfernt. Sie müssen Ihr Gerät erneut an der UMS registrieren.

Menüpfad: **UMS Web App > Geräte > Auf Werkseinstellungen zurücksetzen**

Um ein Gerät auf die Werkseinstellungen zurückzusetzen, gehen Sie wie folgt vor:

1. Wählen Sie in der **UMS Web App > Geräte** das gewünschte Gerät aus und klicken Sie auf ⋮.
2. Klicken Sie **Auf Werkseinstellungen zurücksetzen**.



3. Bestätigen Sie den Dialog.

4. Bestätigen Sie am Gerät, dass es neu gestartet werden kann, oder warten Sie, bis das Gerät automatisch neu startet.

   Nach dem Neustart wird der Einrichtungsassistent angezeigt und Sie können Ihr Gerät am UMS Server erneut registrieren.

Fernzugriff auf Geräte über das Spiegeln in der IGEL UMS Web App

Sie können den Desktop eines Geräts durch Spiegeln mit VNC auf Ihrem lokalen PC beobachten. Das Spiegeln über die UMS Web App und die UMS Konsole wird für IGEL OS 12- und OS 11-Geräte unterstützt. Weitere Informationen zum Spiegeln über die UMS Konsole finden Sie unter Spiegeln - IGEL OS Desktop über VNC beobachten (see page 481).

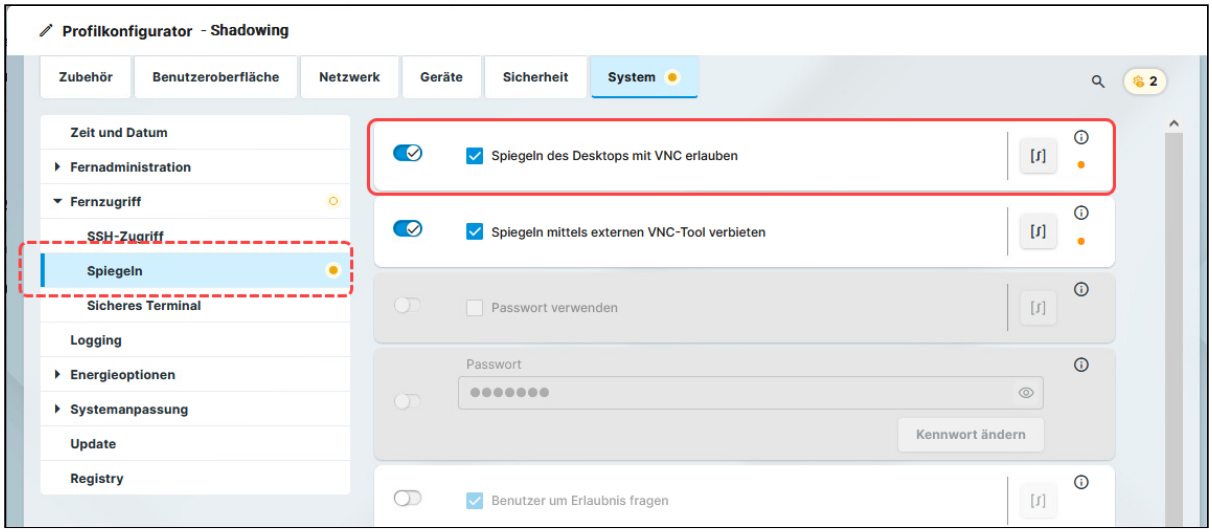
> Für das Spiegeln benötigen Sie **Fernzugriff**-Rechte, die Sie in der UMS Konsole über **[Kontextmenü des Geräts/Geräteverzeichnisses] > Berechtigungen** vergeben können. Siehe Objektbezogene Zugriffsrechte (see page 687).

So spiegeln Sie das IGEL OS 12-Gerät:

1. Erstellen Sie ein Profil für das IGEL OS Base System und gehen Sie zu **System > Fernzugriff > Spiegeln**. Informationen zur Profilerstellung finden Sie unter Profile in der IGEL UMS Web App erstellen und zuweisen (see page 838).

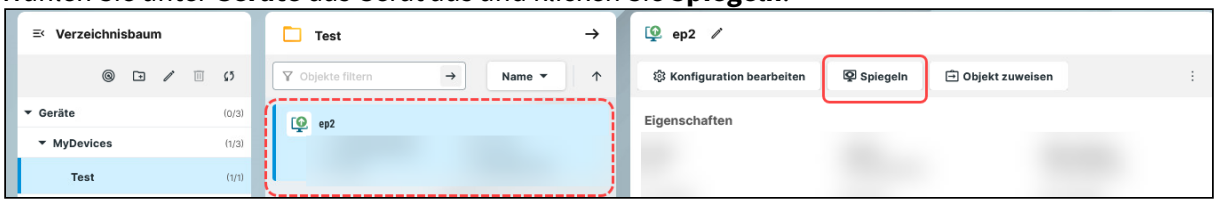
2. Aktivieren Sie **Spiegeln des Desktops mit VNC erlauben** und konfigurieren Sie weitere Einstellungen nach Ihren Bedürfnissen.

   > **Sicheres Spiegeln und IGEL OS 12**
   > Das Shadowing von IGEL OS 12-Geräten über die UMS erfolgt immer über das Unified Protocol und ist daher sicher, d. h. die Kommunikation ist immer verschlüsselt. Standardmäßig wird das Shadowing über das einfache VNC-Protokoll verweigert. Sie können jedoch die Option **Spiegeln mittels externen VNC-Tool verbieten** deaktivieren, wenn Sie möchten, dass die Geräte von einem externer VNC Viewer (see page 485) über das einfache VNC-Protokoll beschattet werden können.



3. Speichern Sie die Einstellungen und weisen Sie das Profil den gewünschten Geräten zu.

4. Wählen Sie unter **Geräte** das Gerät aus und klicken Sie **Spiegeln**.



Die Anfrage für das Spiegeln wird an das Gerät gesendet. Wenn Sie **Benutzer um Erlaubnis fragen** aktiviert haben, muss der Benutzer die Anfrage für das Spiegeln erst akzeptieren.

Geräteeinstellungen als Profil in der IGEL UMS Web App exportieren

In der IGEL Universal Management Suite (UMS) können Sie die Einstellungen von Geräten exportieren. In der exportierten Datei werden alle geänderten Einstellungen gespeichert, d.h. alle Einstellungen, die von den Standardwerten abweichen, unabhängig davon, ob sie über die UMS Profile oder lokal auf dem Gerät konfiguriert sind.

Das Exportieren von Geräteeinstellungen kann für Supportzwecke notwendig sein oder wenn Sie diese später als Profil z. B. in eine andere UMS-Installation importieren möchten.

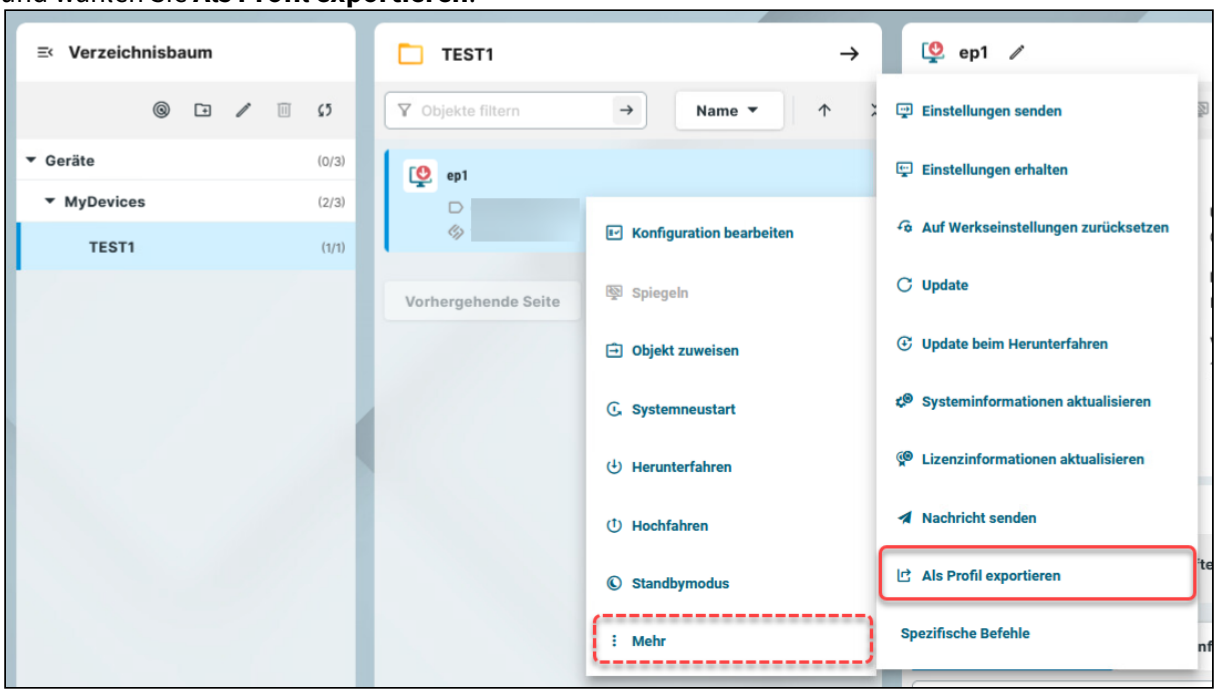
> In der UMS Web App können Sie die Geräteeinstellungen nur für IGEL OS 12-Geräte exportieren. Wenn Sie die Einstellungen von IGEL OS 11-Geräten exportieren möchten, siehe Geräteeinstellungen in der IGEL UMS exportieren (see page 470).

Wenn Sie lediglich Profile exportieren möchten, siehe Profile in der IGEL UMS Web App exportieren und importieren (see page 852).

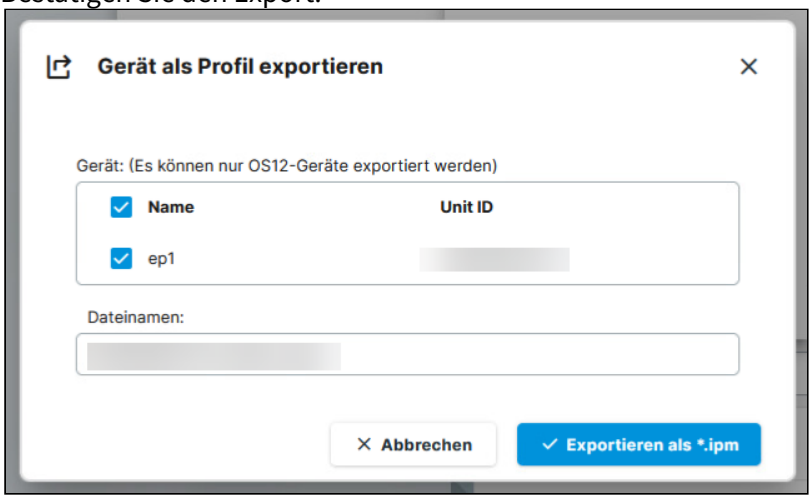
Menüpfad: **UMS Web App > Geräte > [Name des Geräts] > Als Profil exportieren**

So exportieren Sie die Einstellungen von Geräten:

1. Klicken Sie in der **UMS Web App > Geräte** mit der rechten Maustaste auf das gewünschte Gerät und wählen Sie **Als Profil exportieren**.



2. Geben Sie den gewünschten **Dateinamen** an.
3. Bestätigen Sie den Export.



Die Geräteeinstellungen werden als `.ipm`-Datei gespeichert, die auch die Metadaten der IGEL OS Apps enthält, auf denen diese Geräteeinstellungen basieren. Daher ist es nicht notwendig, die benötigten Apps / App-Versionen zusätzlich vom IGEL App Portal (oder aus der UMS) zu importieren.

> Wenn in der UMS, in die Sie die exportierte Datei importieren, die Funktion UMS as an Update Proxy aktiviert ist, aber der Fallback zum App Portal deaktiviert ist, benötigen Sie dennoch die Binärdateien von Apps, siehe Configuring Global Settings for the Update of IGEL OS Apps (see page 889).

Sie können nun die exportierte Datei als Profil importieren, siehe Profile in der IGEL UMS Web App exportieren und importieren (see page 852).

> Alle Passwörter werden entfernt, d.h. in der exportierten Datei durch einen Platzhalter ersetzt. Wenn Sie die exportierten Geräteeinstellungen später als Profil importieren, werden keine Passwörter übernommen. Sie müssen die Passwörter neu setzen.

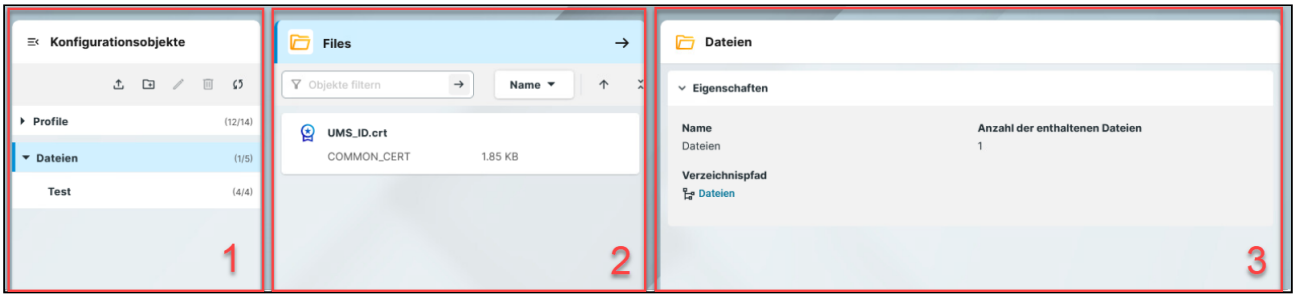
Konfiguration - Zentralisierte Verwaltung von Geräteeinstellungen in der IGEL UMS Web App

Im Bereich **Konfiguration** des IGEL Universal Management Suite (UMS) Web App können Sie Konfigurationsobjekte wie Profile und Dateien erstellen und verwalten, um die zentrale Verwaltung von Geräteeinstellungen zu unterstützen.

Nähere Informationen zu Profilen finden Sie unter Profile in der IGEL UMS (see page 365).

Nähere Informationen zu Dateien finden Sie unter Dateien - Dateien am IGEL UMS Server registrieren und zu Geräten übertragen (see page 529).

Menüpfad: **UMS Web App > Konfiguration**



1	Konfigurationsobjekte Verzeichnisbaum	Sie können Ihre Konfigurationsobjekte strukturieren, indem Sie eine Verzeichnisstruktur unter **Profile**, **Prioritätsprofile** und **Dateien** in der Baumstruktur der **Konfigurationsobjekte** erstellen. Der Verzeichnisbaum zeigt alle erstellten Objektverzeichnisse und -unterverzeichnisse an. Das Format (x/y) gibt 1) die Anzahl der direkt im Verzeichnis enthaltenen Objekte und 2) die Gesamtzahl der Objekte im Verzeichnis und allen Unterverzeichnissen dieses Verzeichnisses an.
2	Objektliste	Wenn Sie ein Verzeichnis in der Baumstruktur auswählen, zeigt die Objektliste alle in diesem Verzeichnis enthaltenen Objekte an.

3	Management-Panel	Der Inhalt des Fensters ändert sich je nach ausgewähltem Element. • Wenn Sie ein Verzeichnis in der Baumstruktur auswählen, zeigt das Panel Verzeichnisinformationen an. Hier finden Sie die **Eigenschaften** des ausgewählten Verzeichnisses, z. B. **Name** und **Verzeichnispfad**. • Wenn Sie ein Objekt aus der Objektliste auswählen, zeigt das Panel die Details des ausgewählten Objekts und alle Funktionen für die Verwaltung des Objekts an. Einzelheiten finden Sie in den Abschnitten Profile Management (see page 831) und File Management (see page 836).

Priority Profile müssen erst in der UMS Konsole unter **UMS Administration > Globale Konfiguration > UMS Features** aktiviert werden, siehe Priority Profile in der IGEL UMS (see page 413). Der Knoten **Priority Profile** wird unter **UMS Web App > Konfiguration** angezeigt. Danach können Sie Priority Profile auf die gleiche Weise wie die Standardprofile erstellen, siehe Profile in der IGEL UMS Web App erstellen und zuweisen (see page 838).

Strukturierungsmaßnahmen

Sie haben die folgenden Möglichkeiten, Ihre Objekte zu strukturieren:

▶ Um ein Verzeichnis zu erstellen, klicken Sie  .

▶ Um ein Verzeichnis umzubenennen, klicken Sie  .

▶ Um ein Verzeichnis zu löschen, klicken Sie  . Derzeit können nur leere Verzeichnisse gelöscht werden.

▶ Um die Liste der Unterverzeichnisse eines Verzeichnisses zu erweitern/zu verkleinern, klicken Sie auf das Pfeilsymbol neben dem Verzeichnisnamen oder doppelklicken Sie auf das Verzeichniselement.

▶ Um das Objekt in ein anderes Verzeichnis zu verschieben, wählen Sie das Objekt aus und verschieben Sie es per Drag & Drop in das gewünschte Verzeichnis.

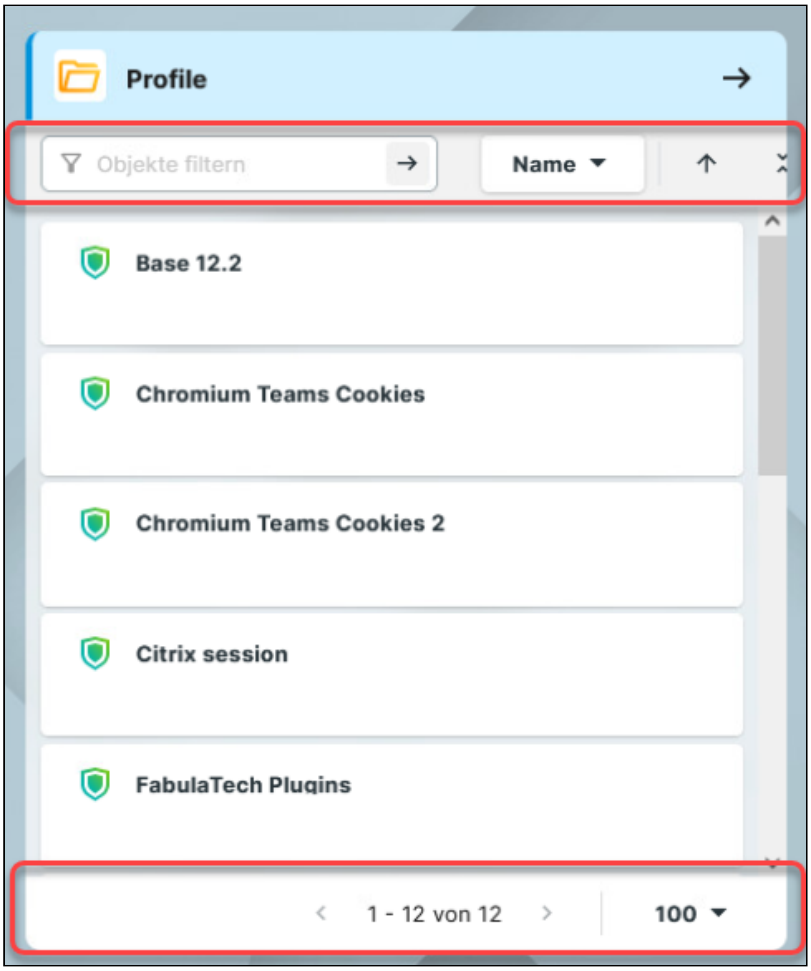
▶ Um die Baumstruktur der Konfigurationsobjekte zu aktualisieren, klicken Sie auf  .

▶ Um das Verzeichnis in ein anderes Verzeichnis zu verschieben, wählen Sie das Verzeichnis aus und verschieben Sie es per Drag & Drop in das gewünschte Verzeichnis oder verwenden Sie [Strg + X], [Strg + V].

Sie können Dateiverzeichnisse nur innerhalb von **Dateien** und Profilverzeichnisse nur innerhalb von **Profilen** verschieben.

Das Kopieren von Objekte in der UMS Web App ist derzeit nicht möglich, stattdessen können Sie die Funktion zum Exportieren und Importieren von Profilen verwenden. Siehe Profile in der IGEL UMS Web App exportieren und importieren (see page 852).

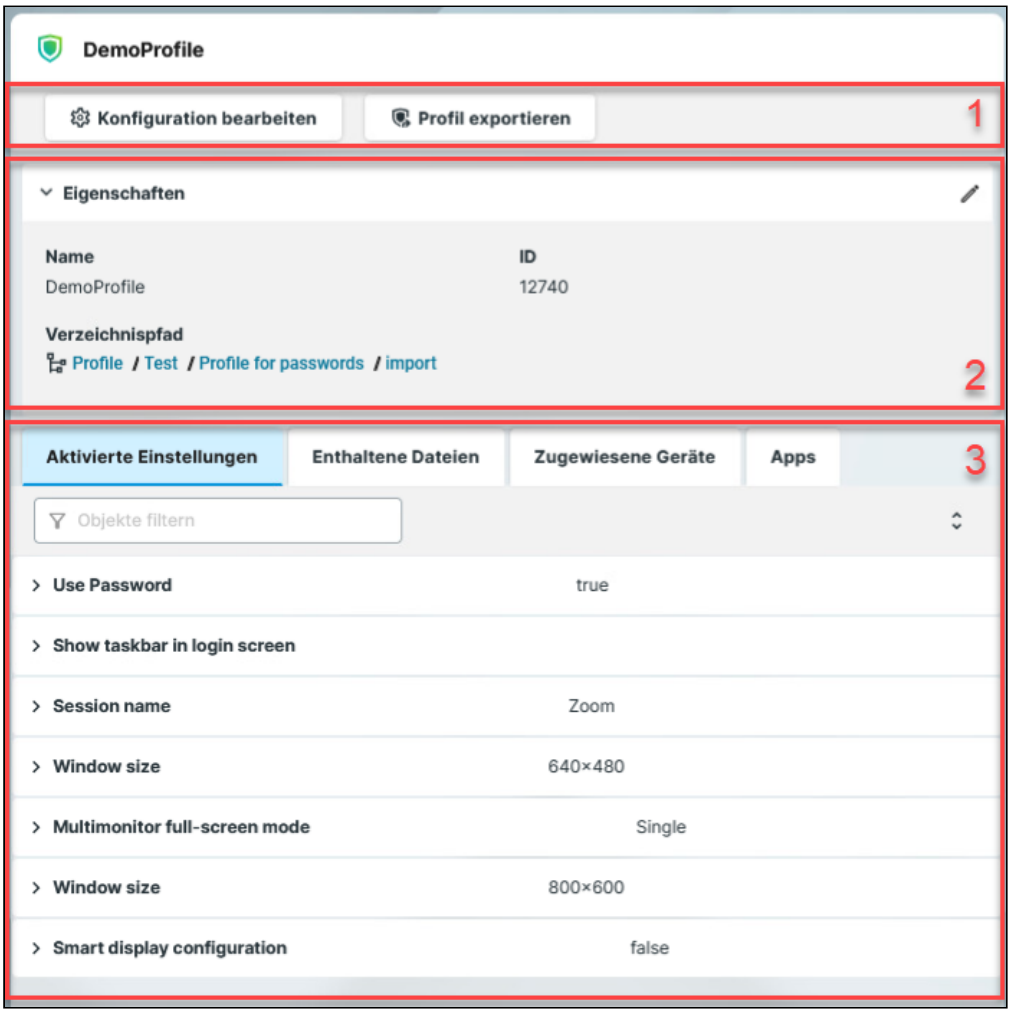
Maßnahmen in der Objektliste



Sie können die aufgelisteten Objekte mit den folgenden Aktionen bearbeiten:

- Verwenden Sie den Freitextfilter, um nach Objekten zu filtern, die den Text in ihrem Namen enthalten
- Profile nach **Name** und **Version** sortieren
- Dateien nach **Name** und **Größe** sortieren
- Ein- und Ausklappen der Objektdetails
- Verwenden Sie das Paging für die Navigation in der Objektliste
- Legen Sie die Anzahl der Objekte fest, die auf einer Seite angezeigt werden sollen

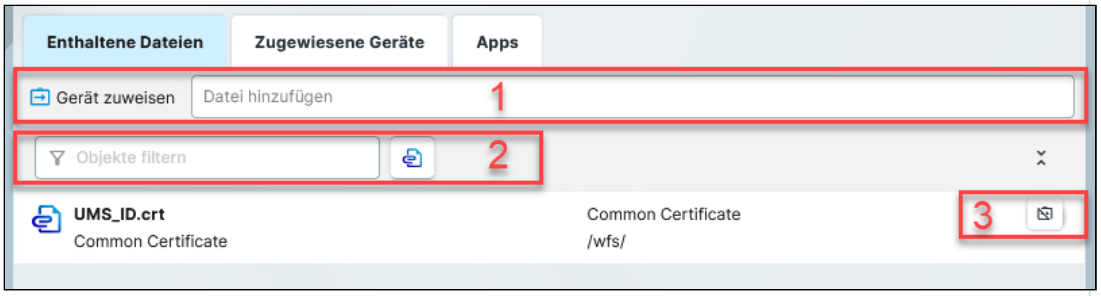
Profile Management Panel

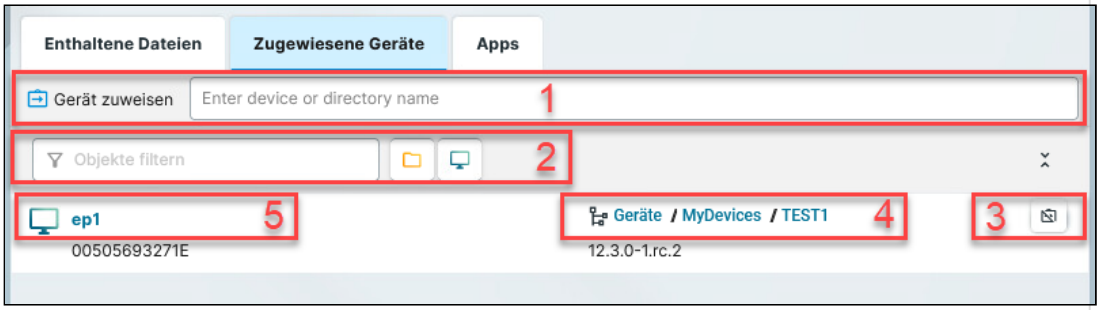


1	Aktionsschaltflächen	▶ Um die Konfigurationsparameter eines Profils zu bearbeiten, doppelklicken Sie auf das Profil in der Objektliste, oder wählen Sie das Profil aus und klicken Sie im Informationsfenster auf **Konfiguration bearbeiten**. ▶ Um das Profil zu exportieren, klicken Sie auf **Profil exportieren**.

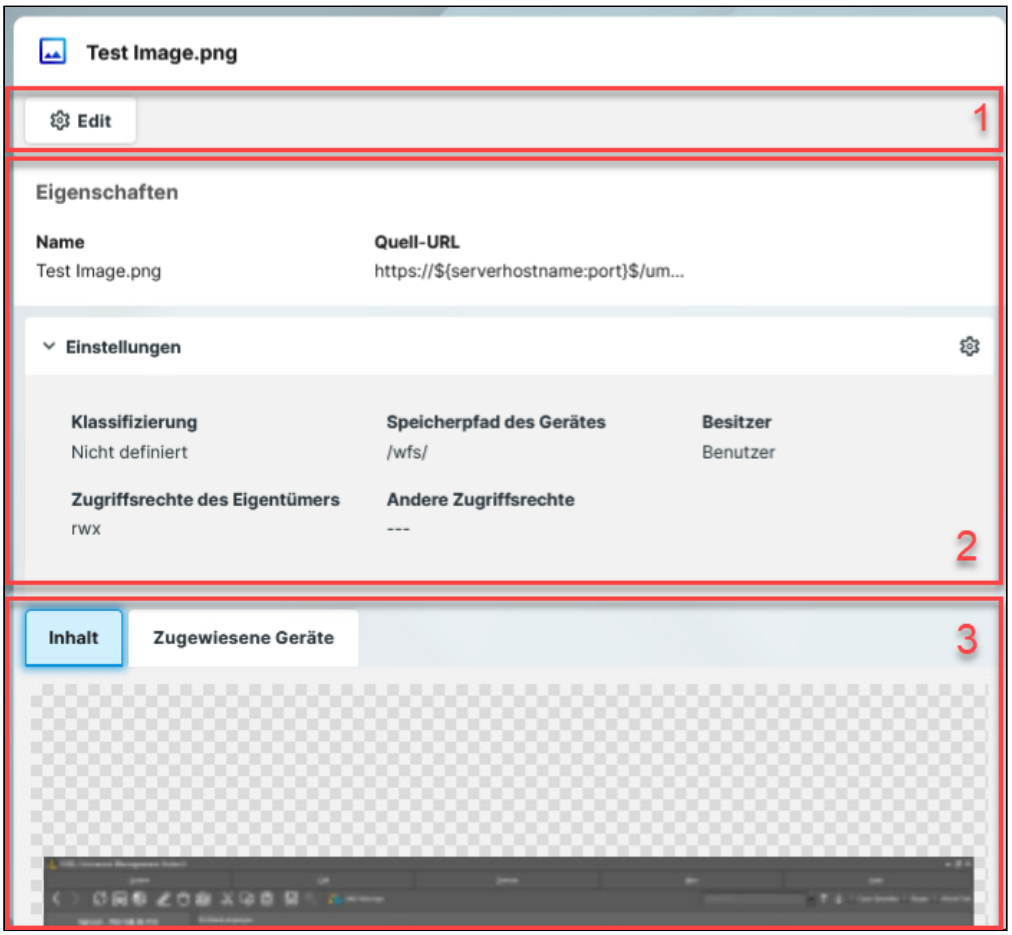
2	Profilinformationen	Bei Profilen zeigt das Informationsfeld die **Eigenschaften** des ausgewählten Profils an, z. B. den **Namen**, die **Version**, auf der es basiert (nur bei IGEL OS 11 Profilen), usw. **ID** Profil-ID. Wenn mehrere Profile einem Gerät gleichrangig zugewiesen sind, hat das neuere Profil, mit der höheren Profil-ID, Priorität. Nähere Informationen zur Priorisierung von Profilen finden Sie unter Wirkungsordnung von Profilen (see page 399) und Priorisierung von Profilen in der IGEL UMS (see page 398). **Verzeichnispfad** Der vollständige Verzeichnispfad für das ausgewählte Profil Um die Eigenschaften zu bearbeiten, klicken Sie auf  .  Die Option **Sitzungen überschreiben** sollte nur in Ausnahmefällen aktiviert werden. Mit dieser Option können Sie freie Instanzen (see page 369) aller anderen Profile überschreiben. Detaillierte Informationen zu dieser Option finden Sie unter Profile in der IGEL UMS erstellen (see page 372).

3	Aktivierte Einstellungen	Zeigt alle Konfigurationseinstellungen an, die im ausgewählten Profil aktiviert sind. **Schlüssel**: Schlüssel des Konfigurationsparameters ▶ Klicken Sie das i-Symbol, um den Tooltip zu öffnen. **Name**: Name des Konfigurationsparameters, wie er im IGEL Setup und im Konfigurationsdialog in der UMS Konsole angezeigt wird. **Wert**: Ein Wert, der für den Parameter gesetzt wurde. Alle Passwortwerte werden anonymisiert. ▶ Wenn ein Parameter einen Wert von einem Templateschlüssel erhält (siehe Templateprofile in der IGEL UMS (see page 416)), klicken Sie , um zu dem entsprechenden Templateschlüssel zu springen. ⚠ Aktivierte Einstellungen für die neu erstellten Profile sowie Einstellungsänderungen werden in der UMS Web App unter **Aktivierte Einstellungen** nicht sofort angezeigt, sondern erst nach dem nächsten Reindizieren, das in diesem Fall mit einem eintägigen Intervall durchgeführt wird.
	Templateschlüssel	Zeigt die im Profil verwendeten Templateschlüssel an, siehe Templateprofile in der IGEL UMS (see page 416) und Templateschlüssel in Profilen verwenden (see page 427). **Templateschlüssel**: Name des Templateschlüssels **Parameter**: Schlüssel des Konfigurationsparameters, für den ein Templateschlüssel konfiguriert ist **Templateausdruck**: Konfigurierter Templateschlüssel Beispiel für einen Templateausdruck: `SSH on §{MAC}` – statischer Templateschlüssel, der den Namen für die SSH-Sitzung konfiguriert, der sich aus "SSH on" und der MAC-Adresse des Endgeräts zusammensetzt

Enthaltene Dateien	Zeigt alle Dateien an, die dem ausgewählten Profil zugeordnet sind. Dateien sollten zuerst in der UMS Konsole hinzugefügt werden. Details zur Dateiübertragung finden Sie unter Dateien - Dateien am IGEL UMS Server registrieren und zu Geräten übertragen (see page 529).  1: Ermöglicht es, dem Profil die Datei schnell hinzuzufügen. Um die Option zu verwenden, sollten Sie den Dateinamen oder dessen Teil bereits kennen. 2: Filtert die dem Profil hinzugefügten Dateien nach der eingegebenen Zeichenkette. 3: Entfernt die ausgewählte Datei von dem Profil.

Zugewiesene Geräte	Zeigt alle Geräte an, denen das ausgewählte Profil zugewiesen ist.  1: Ermöglicht es, dem Gerät oder Geräteverzeichnis das ausgewählte Profil schnell zuzuordnen. Um die Option zu verwenden, sollten Sie den Namen des Geräts / Geräteverzeichnisses oder dessen Teil bereits kennen. 2: Filtert die Geräte / Geräteverzeichnisse, die dem ausgewählten Profil zugeordnet sind. Die Filterkriterien werden mit dem Operator *AND* verknüpft. ▶ Klicken Sie , um alle Filter zu entfernen. 3: Entfernt das ausgewählte Gerät / Geräteverzeichnis von dem Profil. 4: Springt zu dem entsprechenden Verzeichnis und zeigt alle **Zugewiesenen Objekte** dafür an. 5: Springt zu dem entsprechenden Gerät und zeigt alle **Zugewiesenen Objekte** dafür an.
Apps	Zeigt an, welche Apps / App-Versionen das ausgewählte OS 12 Profil konfiguriert.

Datei Management Panel



1	Aktionsschaltflächen	▶ Um die Eigenschaften und Einstellungen der Datei zu bearbeiten, klicken Sie auf **Edit**.
2	Datei Information	Bei Dateien zeigt das Informationsfeld die **Eigenschaften** und **Einstellungen** der ausgewählten Datei an, z. B. **Name** und **Quell-URL**. Die Werte werden beim Hochladen der Datei festgelegt und können später bearbeitet werden. Details zu den Einstellungen finden Sie unter Hochladen und Zuweisen von Dateien in der IGEL UMS Web App (see page 855).

3	Inhalt	Zeigt eine Vorschau der über die UMS Web App hochgeladenen Dateien an. Zum Beispiel eine Bildvorschau oder Zertifikatsinhalte.
	Zugewiesene Geräte	Zeigt alle Geräte an, denen die ausgewählte Datei zugewiesen ist. Details zur Dateizuordnung finden Sie unter Hochladen und Zuweisen von Dateien in der IGEL UMS Web App (see page 855).

Profile in der IGEL UMS Web App erstellen und zuweisen

In der IGEL UMS Web App können Sie Profile erstellen, um die Einstellungen für Ihre Geräte zu konfiguriren. Allgemeine Informationen zu Profilen finden Sie unter Profile in der IGEL UMS (see page 365).

Menüpfad: **UMS Web App > Konfiguration**

Profile für IGEL OS 12 und IGEL OS 11 Geräte

- Das Verfahren zur Erstellung von Profilen für IGEL OS 12 Geräte und IGEL OS 11 Geräte ist unterschiedlich. Wenn Sie z. B. Chromium Browser-Einstellungen für Ihre IGEL OS 12 und IGEL OS 11 Geräte konfigurieren möchten, müssen Sie zwei Profile erstellen – ein Profil für OS 12 Geräte und ein anderes für OS 11 Geräte.
- Profile für IGEL OS 12 Geräte können nur in der UMS Web App erstellt und geändert werden. Es ist nicht möglich, sie in der UMS Konsole zu erstellen/bearbeiten.
- Profile für IGEL OS 11 Geräte können in der UMS Konsole und in der UMS Web App erstellt und bearbeitet werden.
- Direkte Zuweisung von OS 12-Profilen zu OS 11-Geräten ist nicht möglich, und umgekehrt. Wenn Sie ein OS 12-Profil einem OS 11-Gerät indirekt zuweisen, d.h. über eine Verzeichnisstruktur, werden die Einstellungen vom OS 12-Profil für das OS 11-Gerät NICHT berücksichtigt (und umgekehrt).

Direkte und indirekte Zuweisung von Objekten in der IGEL UMS

Objekte in der IGEL UMS können direkt oder indirekt zugeordnet werden:

- Direkt zugeordnete Objekte wurden einem einzelnen Gerät oder Ordner zugewiesen.
- Indirekt zugeordnete Objekte wurden über die Ordnerstruktur 'geerbt'.

Ob ein Profil direkt oder indirekt zugewiesen wird, beeinflusst die Priorität eines Profils, siehe Wirkungsordnung von Profilen (see page 399).
Beachten Sie das Folgende:

- Wenn Sie ein Profil einem Verzeichnis zuweisen, ist es **indirekt** jedem Gerät in diesem Verzeichnis zugewiesen, auch den Unterverzeichnissen.
- Wenn Sie ein Gerät nachträglich in dieses Verzeichnis verschieben, wirken sich die Verzeichnisprofile auch auf dieses Gerät aus.
- Wenn Sie einen Gerät aus diesem Verzeichnis entfernen, beeinflusst das Profil dieses Gerät nicht mehr und die lokalen Einstellungen des Geräts werden wieder hergestellt.

Profile für IGEL OS 12-Geräte erstellen

Bevor Sie Profile für IGEL OS 12-Geräte erstellen, müssen Sie die benötigten Apps vom IGEL App Portal importieren; siehe IGEL OS Apps vom IGEL App Portal importieren (see page 869).

Alternativ muss mindestens ein IGEL OS 12-Gerät mit den benötigten Apps bereits am UMS Server registriert sein. Das IGEL OS-Basissystem sowie alle lokal installierten Apps werden dann automatisch von der UMS erkannt. Siehe z.B. Installing IGEL OS Apps Locally on the Device.

Sobald Apps unter **UMS Web App > Apps** aufgelistet sind, können Sie ein Profil erstellen, um Einstellungen für Ihre Geräte zu konfigurieren.

Es gibt zwei Methoden, ein Profil zu erstellen:

- Über **Konfiguration > Konfigurationsbaum > Neues Profil anlegen** (dient zur Konfiguration mehrerer Apps. Ein Profil konfiguriert ALLE Versionen einer App, es sei denn, die Version ist angegeben.)
- Über **Apps > Neues Profil anlegen** (zur schnellen Konfiguration eines Profils für die ausgewählte App).

Profile können derzeit nicht in der UMS Web App gelöscht werden. Verwenden Sie stattdessen die UMS Konsole.

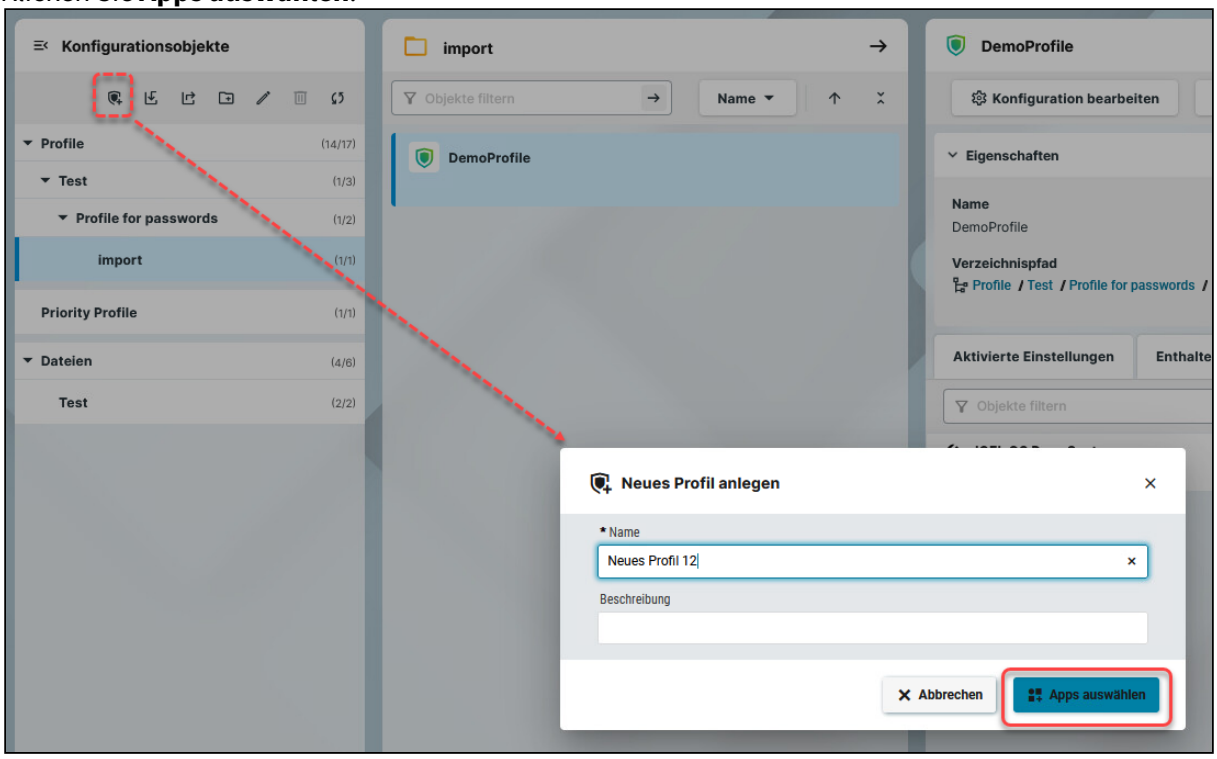
Für Apps, die keine konfigurierbaren Parameter haben (z. B. Codecs), ist es nicht möglich, ein Profil zu erstellen.

Option 1: OS 12-Profil über Konfiguration erstellen

1. Klicken Sie unter **UMS Web App > Konfiguration** auf die Schaltfläche **Neues Profil anlegen**.

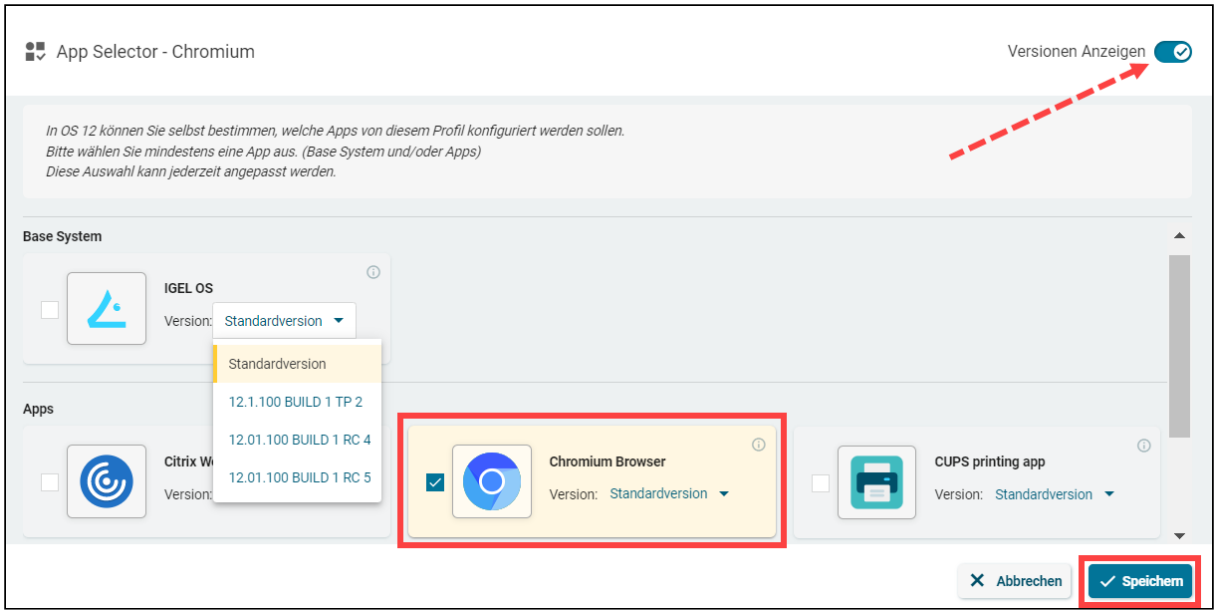
2. Wählen Sie **OS 12** (wird nur angezeigt, wenn OS 11-Geräte in der UMS registriert wurden) und geben Sie den **Namen** des Profils ein. Falls gewünscht, fügen Sie eine **Beschreibung** für das Profil hinzu.

3. Klicken Sie **Apps auswählen**.



4. Wählen Sie im **App Selector** die App(s) aus, die Sie konfigurieren möchten. Es ist IMMER notwendig, mindestens eine App auszuwählen, wenn Sie ein Profil für IGEL OS 12-Geräte erstellen.

> Wenn Sie Profile zur Konfiguration von IGEL OS Base System-Einstellungen (z.B. Corporate Design, SSO, Zubehör usw.) erstellen möchten, bevor eines Ihrer IGEL OS 12-Geräte an der UMS registriert wird, importieren Sie die IGEL OS Base System App. Es wird empfohlen, die neueste App-Version zu verwenden. Allein zum Zweck der Profilerstellung ist die anschließende Zuweisung der IGEL OS Base System App zu einem Gerät / Geräteverzeichnis NICHT erforderlich.



5. Wenn Sie ein Profil für eine bestimmte App-Version konfigurieren möchten, aktivieren Sie **Versionen anzeigen** und wählen Sie die gewünschte Version aus.

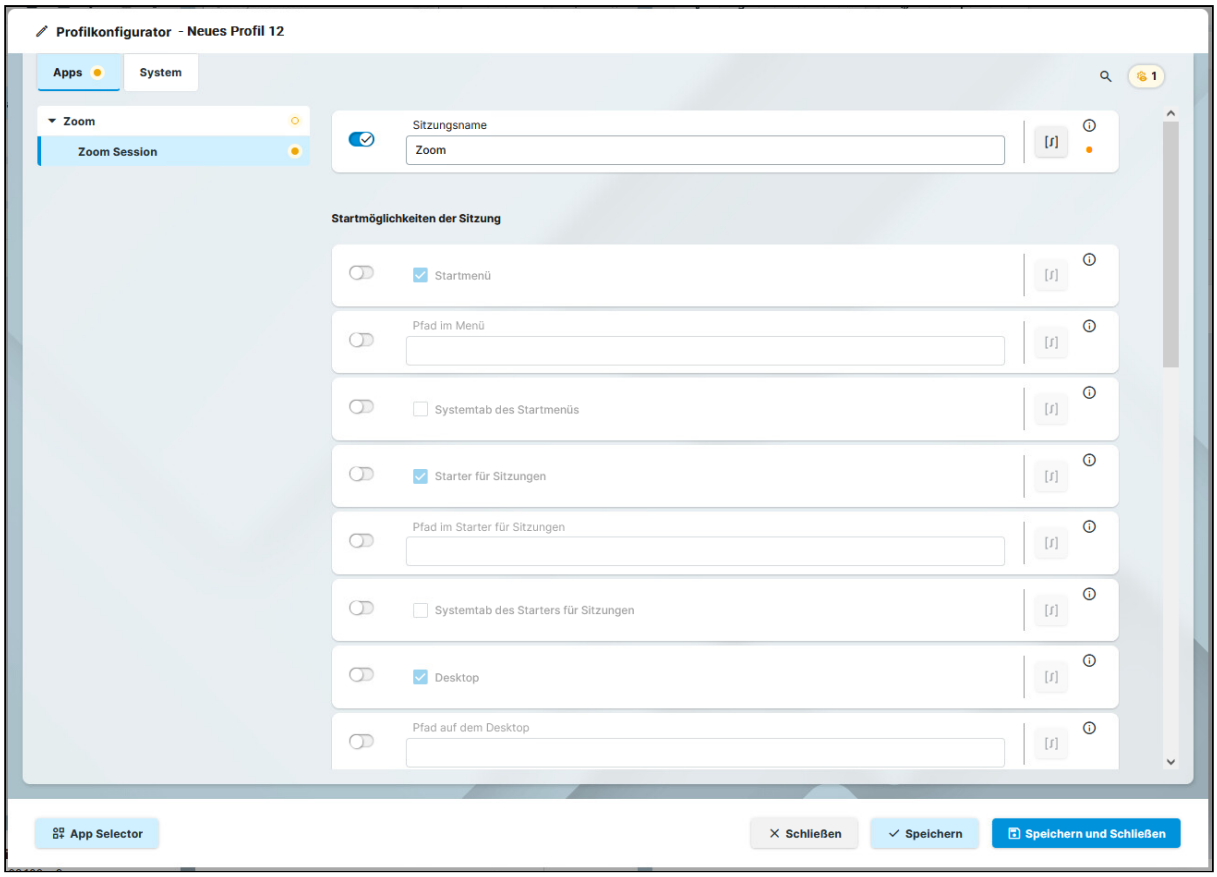
   > Eine hier ausgewählte App-Version wird einem Gerät zugewiesen, siehe Zuordnung von OS 12-Profilen zu Geräten, oder implizite App-Zuweisung über Profile (see page 844).
   > Die Best Practice ist die Verwendung der **Standardversion**, siehe Standardversion einer App in der IGEL UMS festlegen (see page 876).

6. Klicken Sie **Speichern**.
   Das Profil wird gespeichert und unter **Konfiguration > Profile** aufgelistet, auch wenn Sie im nächsten Schritt keine Einstellungen vornehmen werden.

7. Konfigurieren Sie die gewünschten Einstellungen.
   Im Konfigurationsdialog werden nur die Einstellungen angezeigt, die für die ausgewählte(n) App(s) konfiguriert werden können. Wenn Sie den Geltungsbereich des Profils ändern möchten (d. h. neu festlegen möchten, welche Apps im Profil konfiguriert werden sollen), klicken Sie **App Selector**.
    .

	Der Parameter ist inaktiv und wird nicht durch das Profil konfiguriert. **WICHTIG**: Wenn Sie den Parameter deaktivieren, wird der Wert automatisch auf den Standardwert zurückgesetzt.

	Der Parameter ist aktiv und der eingestellte Wert wird durch das Profil konfiguriert.



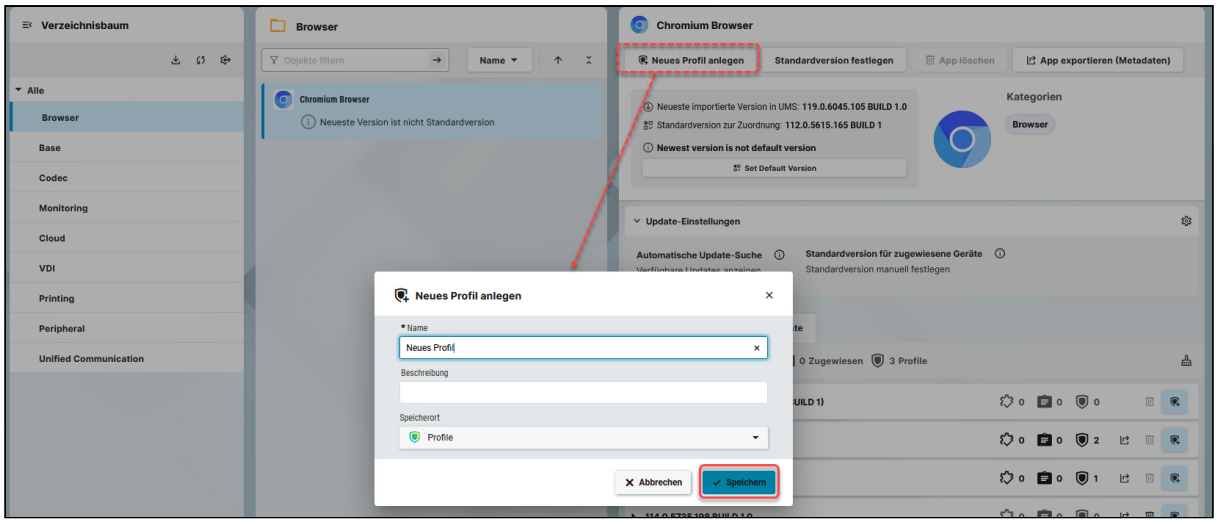
8. Speichern Sie die Änderungen.

9. Weisen Sie das Profil dem gewünschten Gerät / Geräteverzeichnis zu. Siehe Zuordnung von OS 12-Profilen zu Geräten, oder implizite App-Zuweisung über Profile (see page 844).

Option 2: OS 12-Profil über Apps erstellen

Um ein Profil für eine importierte App schnell zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie unter **UMS Web App > Apps** die gewünschte App aus und klicken Sie **Neues Profil anlegen**.

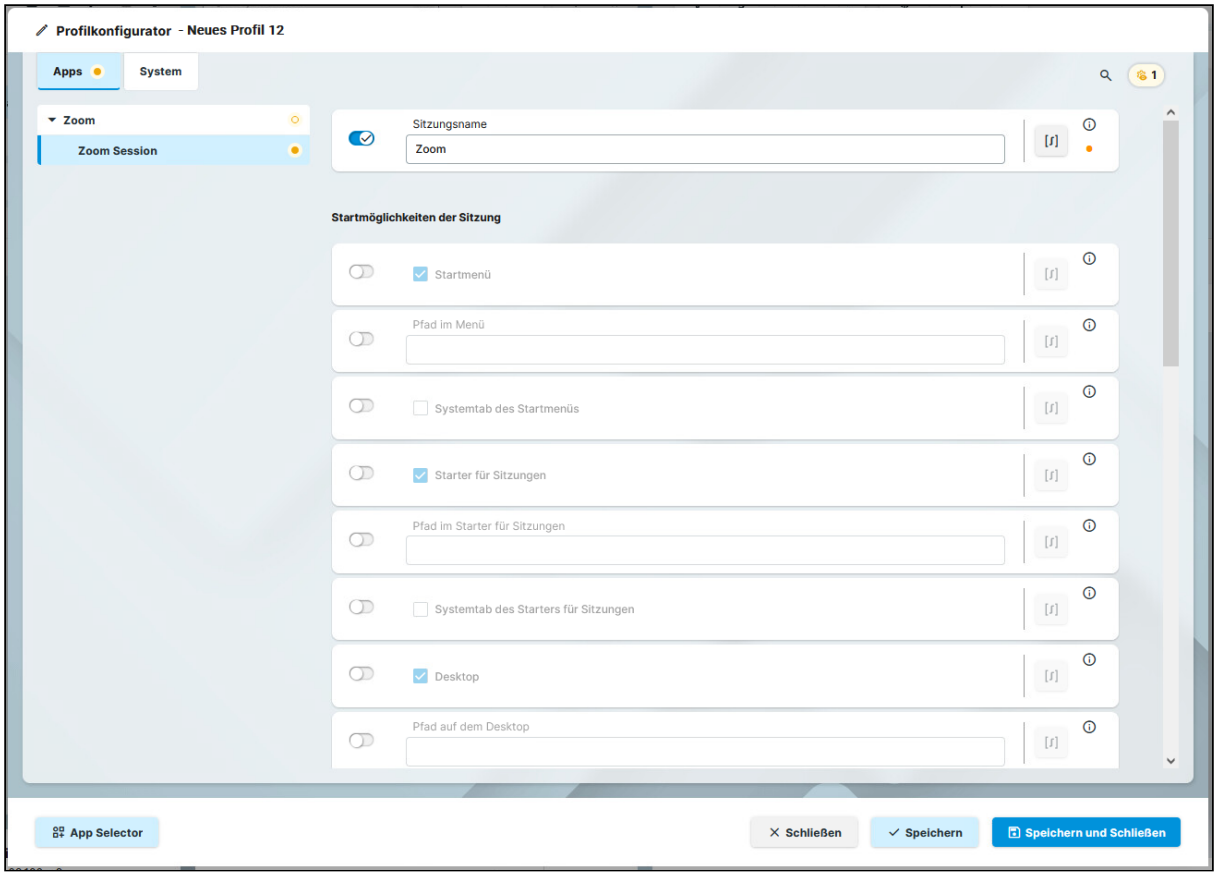


2. Geben Sie den **Namen** des Profils ein und geben Sie unter **Downloadpfad** das gewünschte Verzeichnis für die Speicherung des Profils an. Falls gewünscht, fügen Sie die **Beschreibung** für das Profil hinzu.

3. Klicken Sie **Speichern**.
   Das Profil wird gespeichert und unter **Konfiguration > Profile** aufgelistet, auch wenn Sie im nächsten Schritt keine Einstellungen vornehmen werden.

4. Konfigurieren Sie die gewünschten Einstellungen.
   Im Konfigurationsdialog werden nur die Einstellungen angezeigt, die für die ausgewählte App konfiguriert werden können. Wenn Sie den Geltungsbereich des Profils ändern möchten (d. h. neu festlegen möchten, welche Apps im Profil konfiguriert werden sollen), klicken Sie **App Selector** .

	Der Parameter ist inaktiv und wird nicht durch das Profil konfiguriert. **WICHTIG**: Wenn Sie den Parameter deaktivieren, wird der Wert automatisch auf den Standardwert zurückgesetzt.
	Der Parameter ist aktiv und der eingestellte Wert wird durch das Profil konfiguriert.



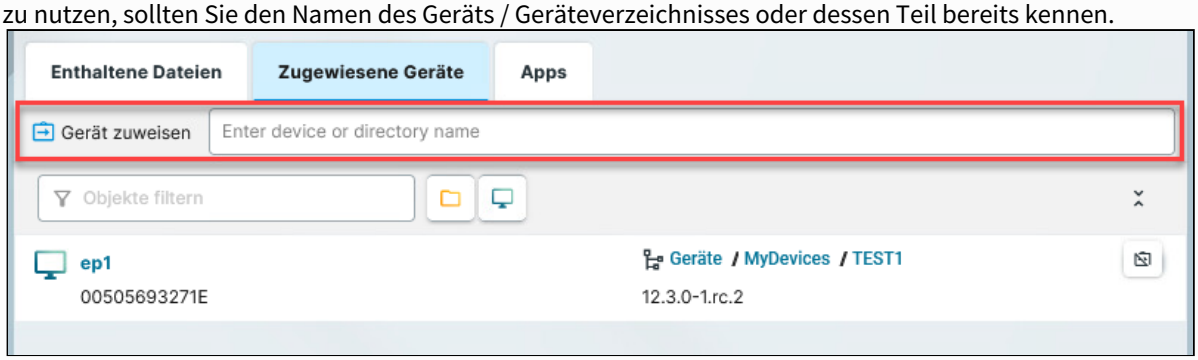
5. Speichern Sie die Änderungen.

6. Weisen Sie das Profil dem gewünschten Gerät / Geräteverzeichnis zu. Siehe Zuordnung von OS 12-Profilen zu Geräten, oder implizite App-Zuweisung über Profile (see page 844).

Zuordnung von OS 12-Profilen zu Geräten, oder implizite App-Zuweisung über Profile

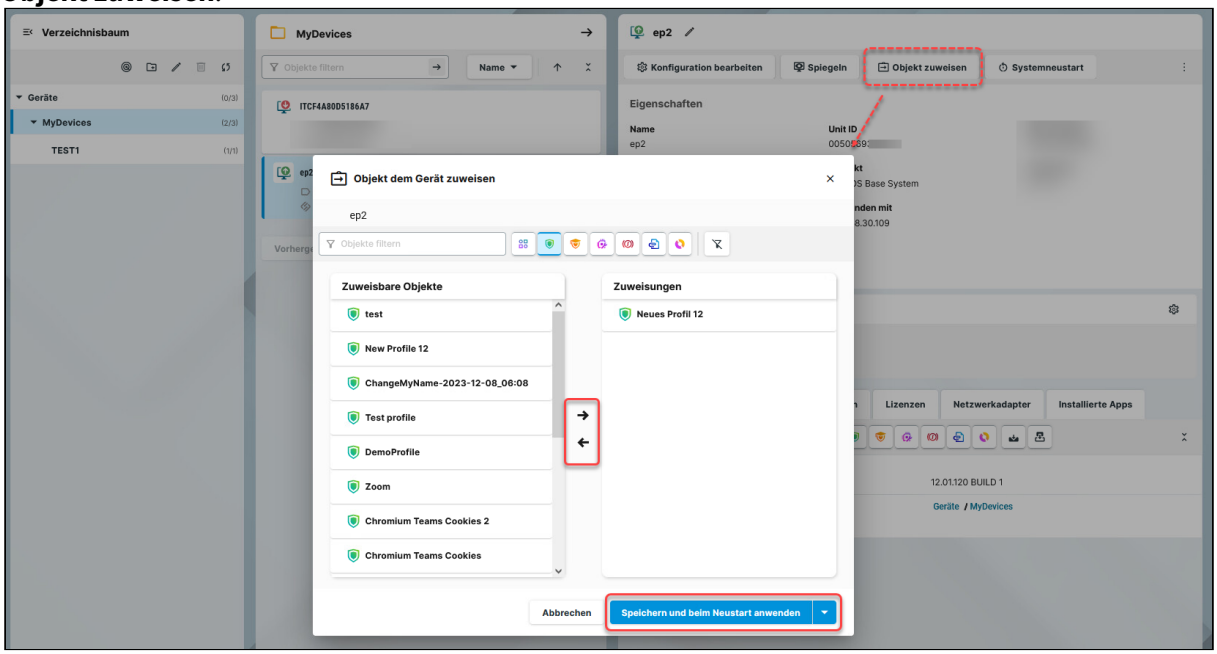
Implizite App-Zuweisung über Profile
Eine App wird einem Gerät automatisch über ein Profil zugewiesen, das diese App konfiguriert.
Ausnahmen: IGEL OS Base System App
Die App-Version, die über die implizite Zuweisung auf dem Gerät installiert wird, wenn mehrere Profile diese App (aber in unterschiedlichen Versionen) konfigurieren, wird durch die Priorisierungsregeln für Profile bestimmt, siehe Priorisierung von Profilen in der IGEL UMS (see page 398) und Zusammenfassung - Priorisierung von IGEL UMS Profilen (see page 411). Beachten Sie, dass die explizit zugewiesene App, d.h. die App / App-Version, die im Dialog **Objekt zuweisen** als Objekt ausgewählt wurde, IMMER die implizit zugewiesene App überschreibt. Siehe Apps zu IGEL OS Geräten über die UMS Web App zuweisen (see page 878).

Um ein Profil einem Gerät / Geräteverzeichnis schnell zuzuweisen, können Sie die Funktion **Gerät zuweisen** unter **Konfiguration > [Name des Profils] > Zugewiesene Geräte** verwenden. Um diese Option zu nutzen, sollten Sie den Namen des Geräts / Geräteverzeichnisses oder dessen Teil bereits kennen.



Um einem Gerät / Geräteverzeichnis Profile zuzuweisen, gehen Sie wie folgt vor:

1. Wählen Sie unter **UMS Web App > Geräte** ein Gerät oder Geräteverzeichnis aus und klicken Sie **Objekt zuweisen**.



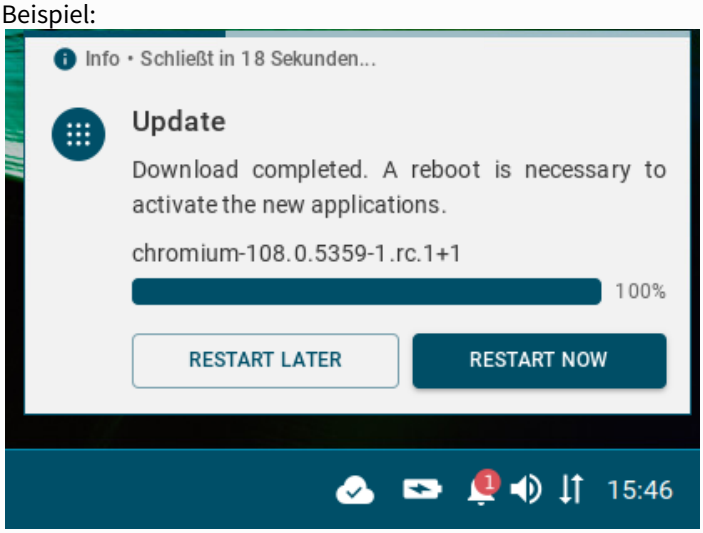
2. Wählen Sie das Profil, das Sie dem Gerät / Geräteverzeichnis zuweisen möchten, und verwenden Sie die Pfeiltaste oder Drag & Drop.

3. Speichern Sie die Änderungen.

4. Entscheiden Sie, wann die Änderungen wirksam werden sollen, und speichern Sie, indem Sie **Speichern und beim Neustart anwenden** oder **Speichern und jetzt anwenden** wählen.

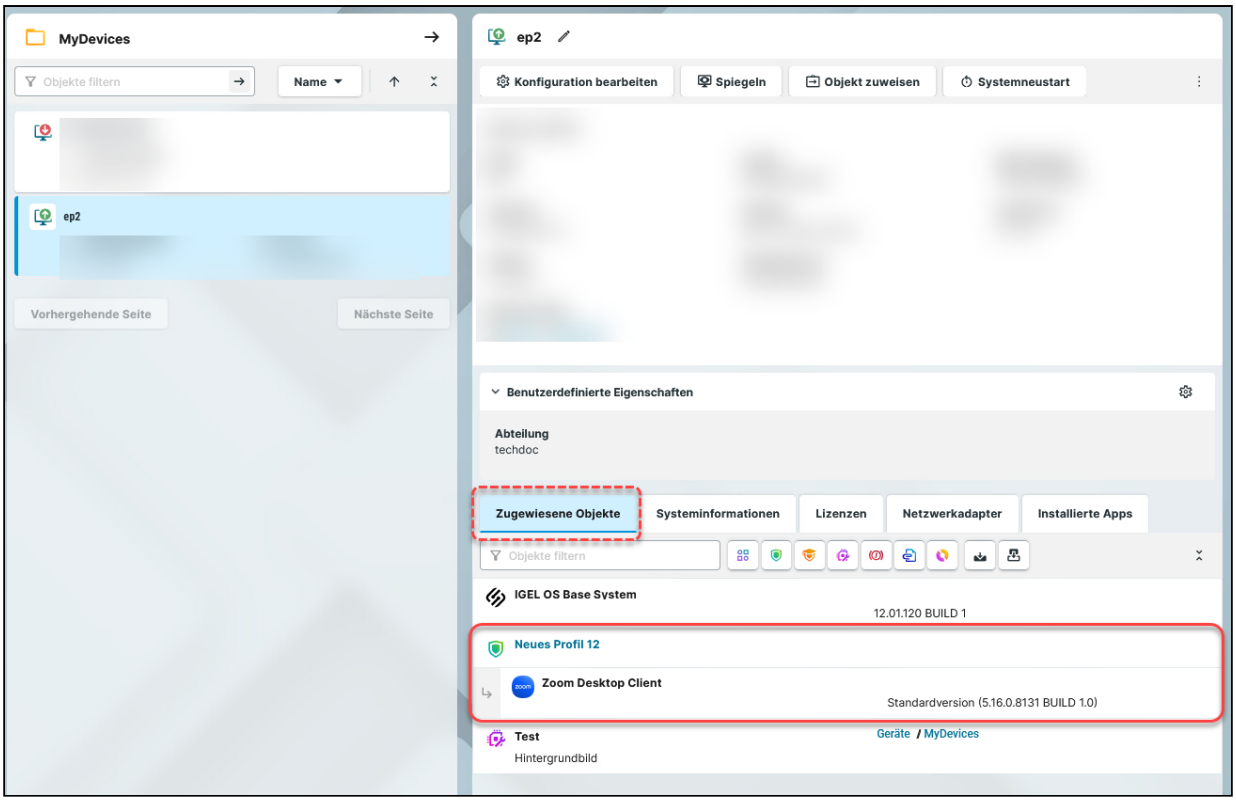
Eine über das Profil zugewiesene App wird auf das Gerät heruntergeladen.

Standardmäßig werden die Apps / App-Versionen beim nächsten Neustart automatisch aktiviert. Der Benutzer erhält eine entsprechende Benachrichtigung.
Beispiel:



Wenn Sie das Background App Update konfiguriert haben, muss stattdessen ein **Update**-Befehl gesendet werden. Weitere Informationen finden Sie unter How to Configure the Background App Update in the IGEL UMS Web App (see page 893).

Das zugeordnete Profil und die App, die dem Gerät über dieses Profil zugewiesen wurde, werden unter **Geräte > Zugewiesene Objekte** angezeigt.



Um die installierten Apps zu überprüfen, gehen Sie zu **Geräte > Installierte Apps**; siehe Checking Installed Apps via the IGEL UMS Web App (see page 882).

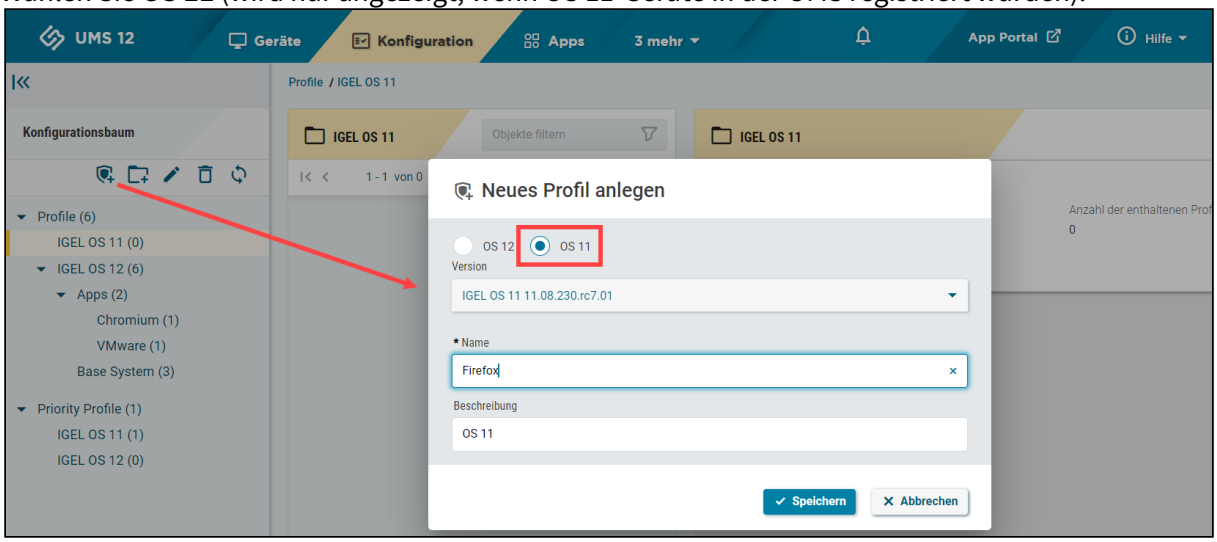
Profile für IGEL OS 11-Geräte erstellen

Wie Sie IGEL OS 11-Profile in der UMS Konsole erstellen können, erfahren Sie unter Profile in der IGEL UMS erstellen (see page 372).

Um ein Profil für IGEL OS 11-Geräte über die UMS Web App zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie unter **UMS Web App > Konfiguration** auf die Schaltfläche **Neues Profil anlegen**.

2. Wählen Sie **OS 11** (wird nur angezeigt, wenn OS 11-Geräte in der UMS registriert wurden).



3. Wählen Sie die **Version** der Firmware aus, auf der das Profil basiert.

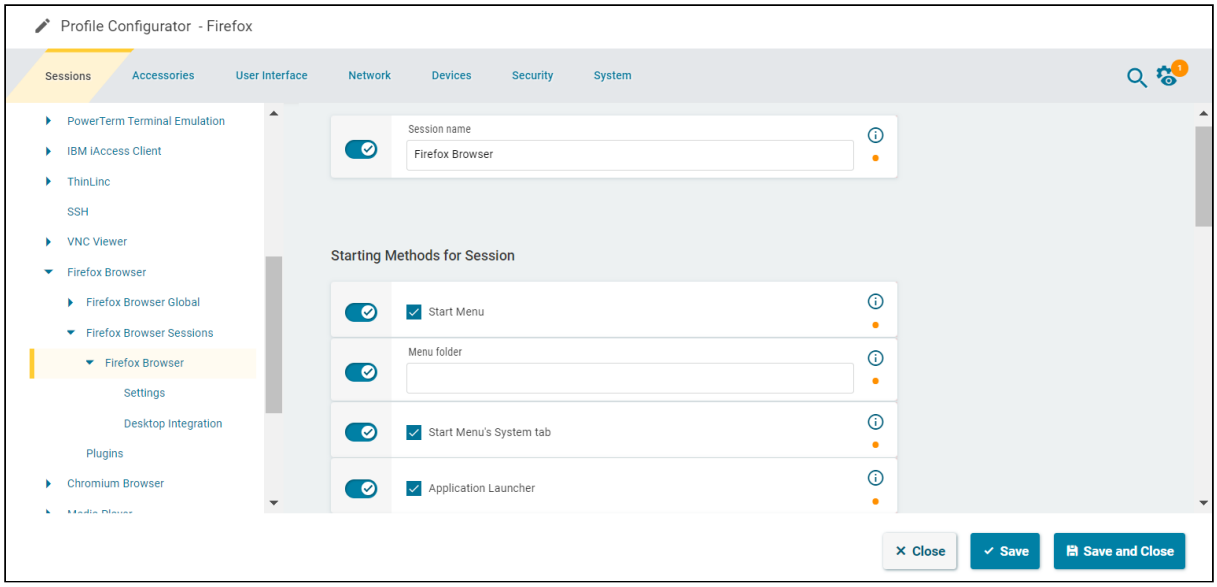
4. Geben Sie den **Namen** des Profils ein.

5. Falls gewünscht, fügen Sie eine **Beschreibung** für das Profil hinzu.

6. Klicken Sie **Speichern**.
   Das Profil wird gespeichert und unter **Konfiguration > Profile** aufgelistet, auch wenn Sie im nächsten Schritt keine Einstellungen vornehmen werden.

7. Konfigurieren Sie die gewünschten Einstellungen.

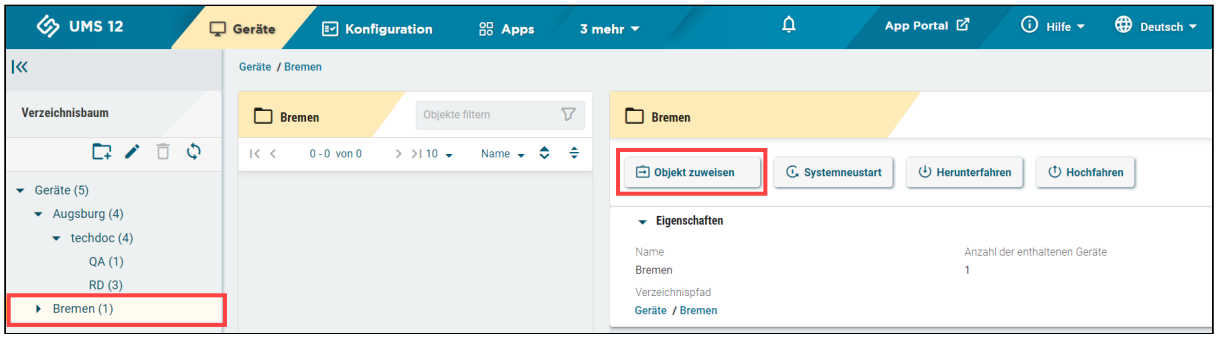
	Der Parameter ist inaktiv und wird nicht durch das Profil konfiguriert. **WICHTIG**: Wenn Sie den Parameter deaktivieren, wird der Wert automatisch auf den Standardwert zurückgesetzt.
	Der Parameter ist aktiv und der eingestellte Wert wird durch das Profil konfiguriert.



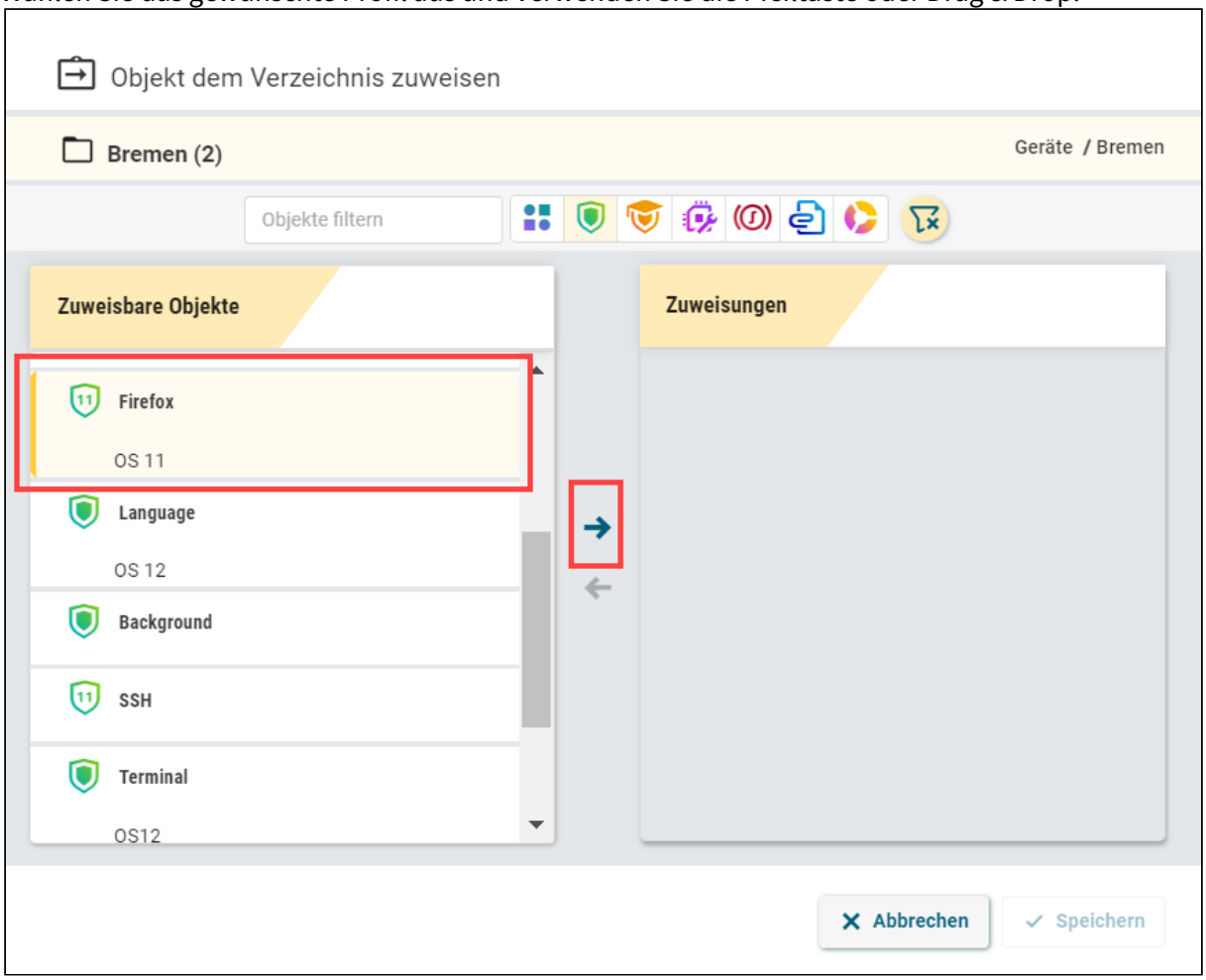
8. Speichern Sie die Änderungen.
9. Weisen Sie das Profil einem Gerät / Geräteverzeichnis zu; siehe die Anweisungen unten.

Zuordnung von OS 11-Profilen zu Geräten

1. Um ein Profil zuzuweisen, gehen Sie zu **Geräte > [Name des Geräts / Geräteverzeichnis] > Objekt zuweisen**.

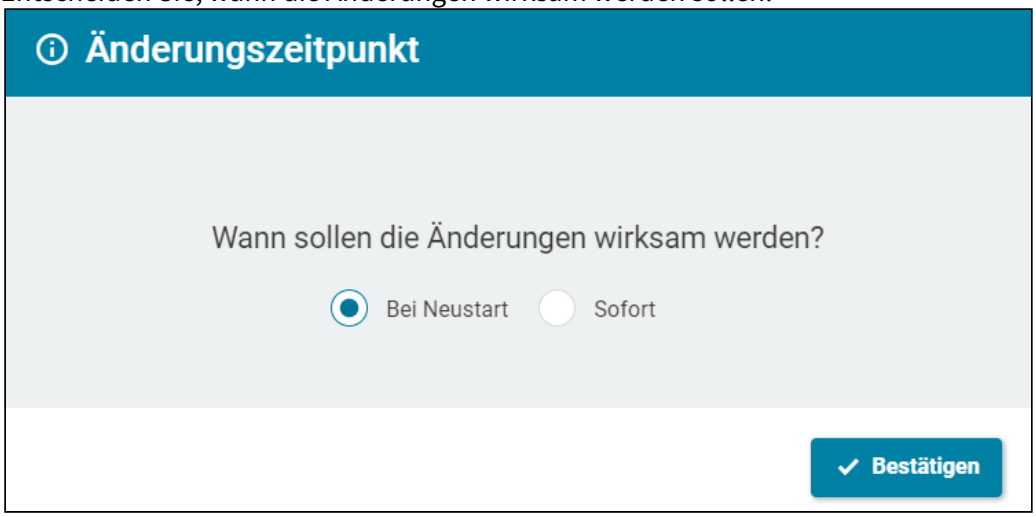


2. Wählen Sie das gewünschte Profil aus und verwenden Sie die Pfeiltaste oder Drag & Drop.



3. Speichern Sie die Änderungen.

4. Entscheiden Sie, wann die Änderungen wirksam werden sollen.



Um ein Profil einem Gerät / Geräteverzeichnis schnell zuzuweisen, können Sie die Funktion **Gerät zuweisen** unter **Konfiguration > [Name des Profils] > Zugewiesene Geräte** verwenden. Um diese Option zu nutzen, sollten Sie den Namen des Geräts / Geräteverzeichnisses oder dessen Teil bereits kennen.

Profile in der IGEL UMS Web App exportieren und importieren

In der IGEL Universal Management Suite (UMS) können Profile samt ihrer Verzeichnisstruktur aus der Datenbank exportiert werden. Dies kann für Backupzwecke oder zum Importieren von Profildaten aus einer UMS Installation in eine andere hilfreich sein.

Alternativ können auch Einstellungen von Geräten als Profile importiert werden; siehe Geräteeinstellungen als Profil in der IGEL UMS Web App exportieren (see page 826).

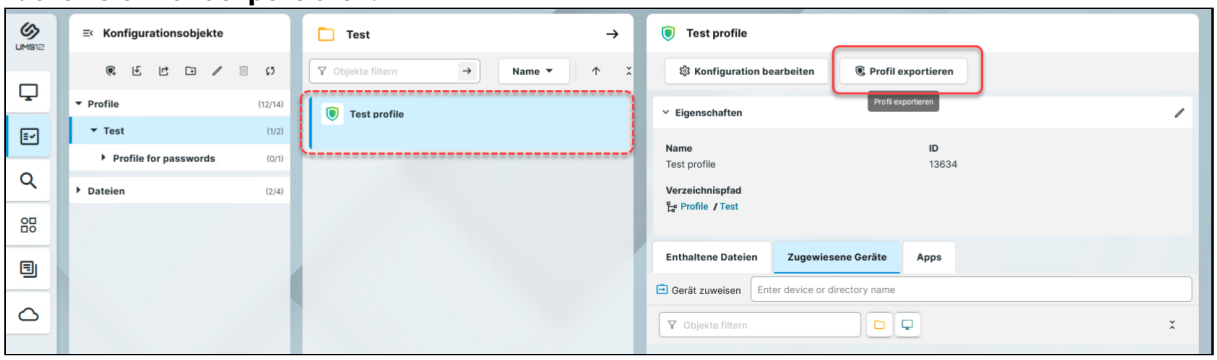
> In der UMS Web App können nur OS 12-Profile exportiert oder importiert werden. Wenn Sie OS 11-Profile exportieren / importieren möchten, siehe Profile exportieren und importieren (see page 390).

Menüpfad: **UMS Web App > Konfiguration > Profil exportieren / Profile importieren**

Profile exportieren

So exportieren Sie ein einzelnes Profil:

1. Wählen Sie unter **UMS Web App > Konfiguration** das gewünschte Profil aus.
2. Klicken Sie **Profil exportieren**.



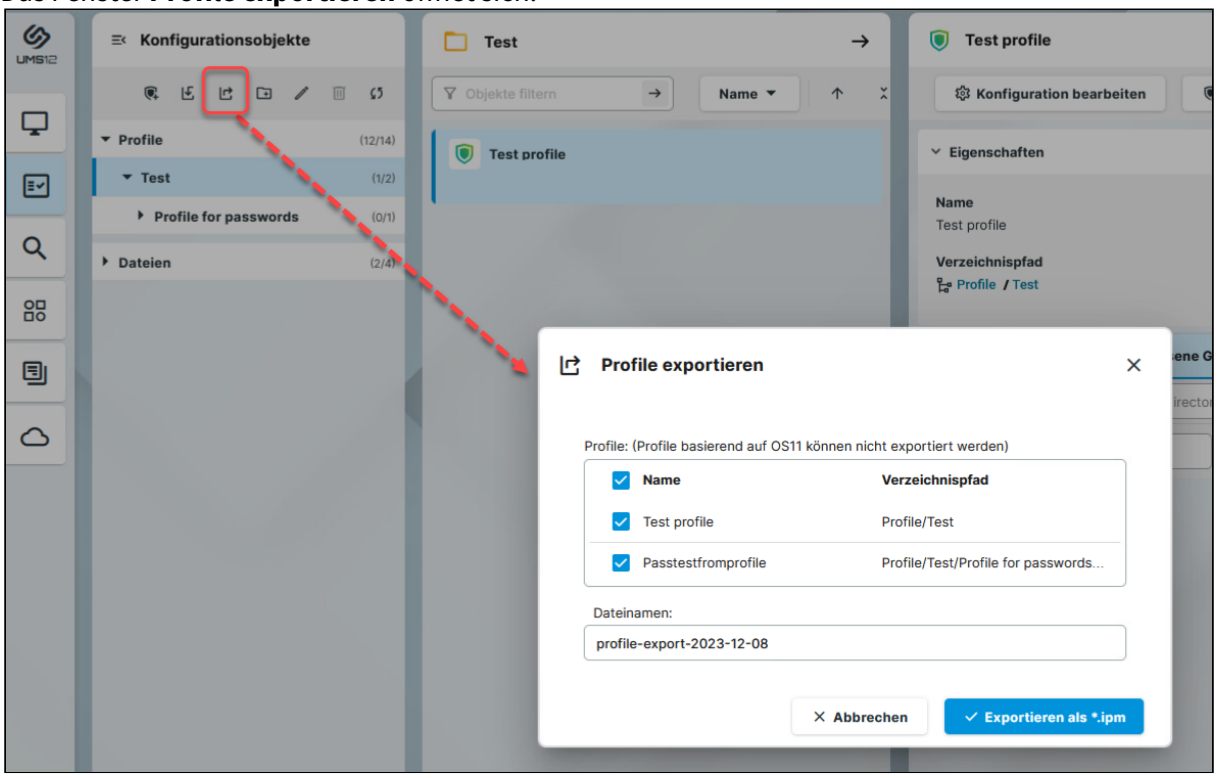
3. Geben Sie den gewünschten **Dateinamen** an.
4. Bestätigen Sie den Export.

So exportieren Sie mehrere Profile in eine Datei:

1. Wählen Sie unter **UMS Web App > Konfiguration** das Verzeichnis **Profile** oder das Verzeichnis, das die Profile enthält, die Sie exportieren möchten.

2. Klicken Sie **Profil exportieren** .

   Das Fenster **Profile exportieren** öffnet sich.



3. Wählen Sie die Profile aus, die Sie exportieren möchten.

4. Geben Sie den **Dateinamen** an.

5. Bestätigen Sie den Export.

Die exportierten Profile werden als `.ipm`-Datei gespeichert, die auch die Metadaten der IGEL OS Apps enthält, auf denen die Profile basieren. Daher ist es nicht notwendig, die benötigten Apps / App-Versionen zusätzlich vom IGEL App Portal (oder aus der UMS) zu importieren.

> Wenn in der UMS, in die Sie die exportierte Datei importieren, die Funktion UMS as an Update Proxy aktiviert ist, aber der Fallback zum App Portal deaktiviert ist, benötigen Sie dennoch die Binärdateien von Apps, siehe Configuring Global Settings for the Update of IGEL OS Apps (see page 889).

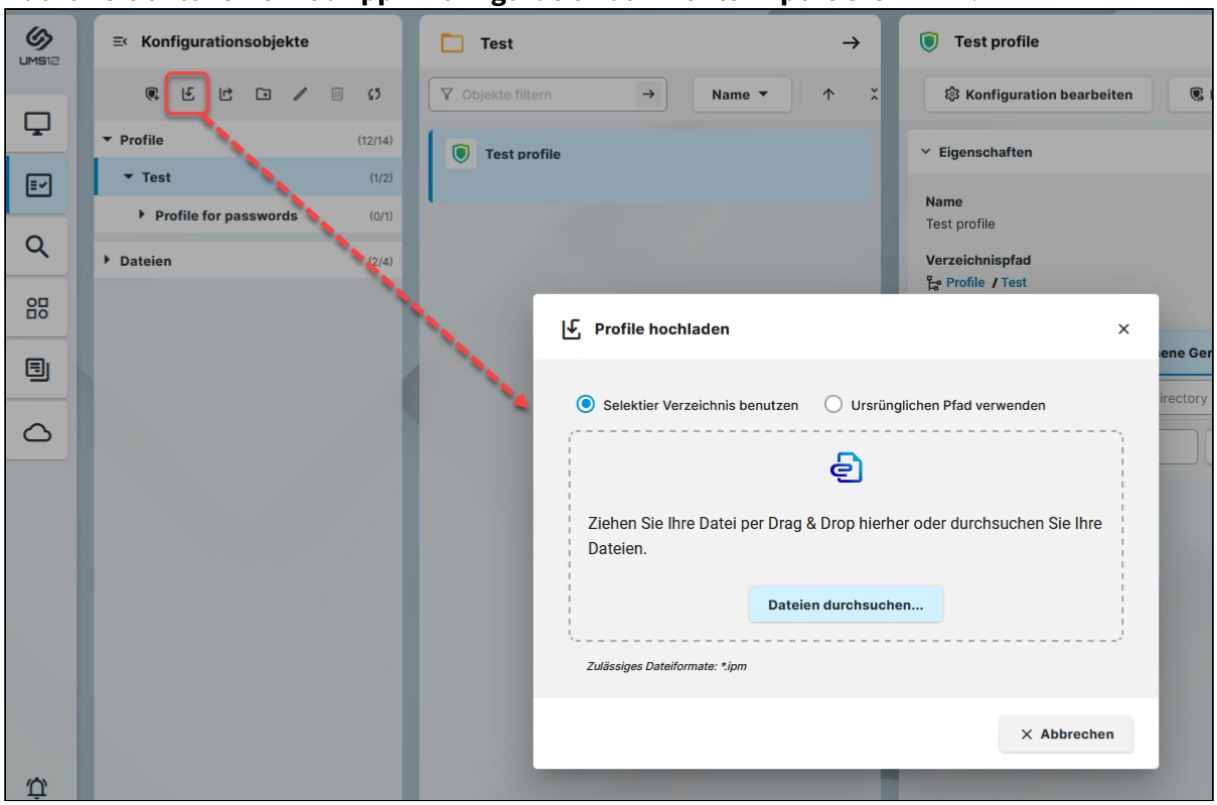
Sie können nun die exportierte Datei wie unten beschrieben importieren.

> Alle Passwörter werden entfernt, d.h. in der exportierten Datei durch einen Platzhalter ersetzt. Wenn Sie die exportierten Geräteeinstellungen später als Profil importieren, werden keine Passwörter übernommen. Sie müssen die Passwörter neu setzen.

Profile importieren

So importieren Sie Profile:

1. Klicken Sie unter **UMS Web App > Konfiguration** auf **Profile importieren** .



2. Wählen Sie aus, ob die Profile in das markierte Verzeichnis abgelegt werden sollen oder ob der ursprüngliche Verzeichnispfad der Profile beibehalten werden soll.

3. Wählen Sie die Datei aus, die Ihr(e) Profil(e) enthält.

4. Wenn das Hochladen abgeschlossen ist, bestätigen Sie den Import.
   Die entsprechenden Profile sowie die Metadaten der IGEL OS Apps, die von diesen Profilen konfiguriert werden, werden in die UMS importiert.
   Bei Bedarf können Sie nun die Profile Ihren Endgeräten zuweisen.

> Profile können als Priority Profile importiert werden (und umgekehrt).

Hochladen und Zuweisen von Dateien in der IGEL UMS Web App

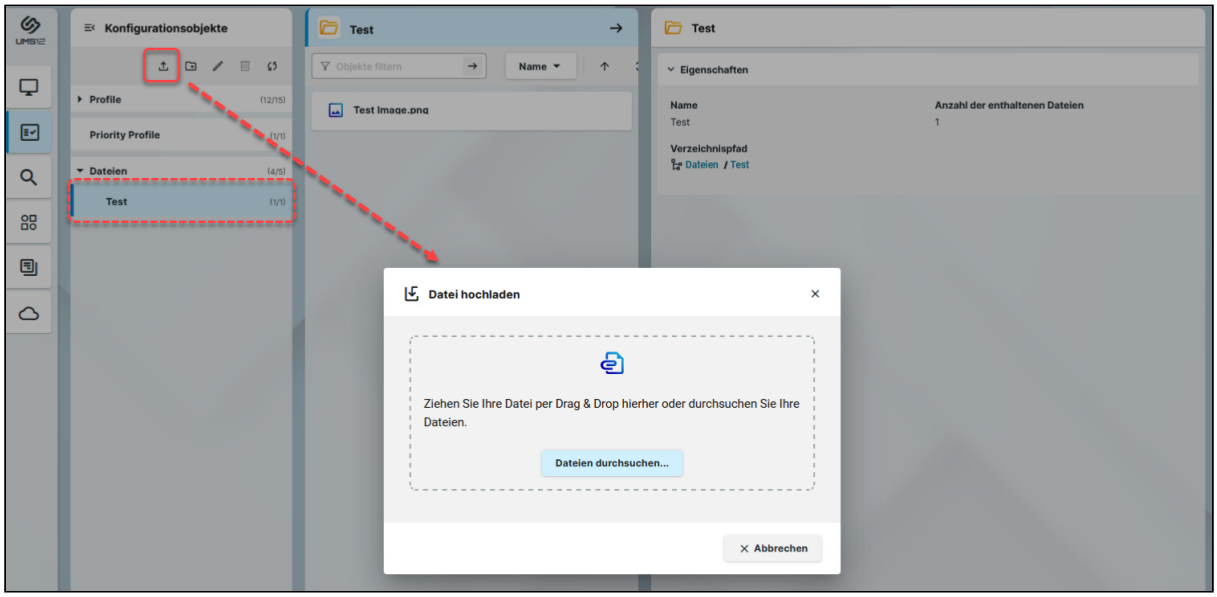
In der IGEL Universal Management Suite (UMS) Web App können Sie Dateien als Konfigurationsobjekte hochladen. Anschließend können Sie diese Dateien durch Zuweisung an Ihre Geräte verteilen. Für Informationen über Konfigurationsobjekte siehe Konfiguration - Zentralisierte Verwaltung von Geräteeinstellungen in der IGEL UMS Web App (see page 828).

> Dateien können derzeit nicht in der UMS Web App gelöscht werden. Verwenden Sie stattdessen die UMS-Konsole.

Menüpfad: **UMS Web App > Konfiguration**

Hochladen von Dateien

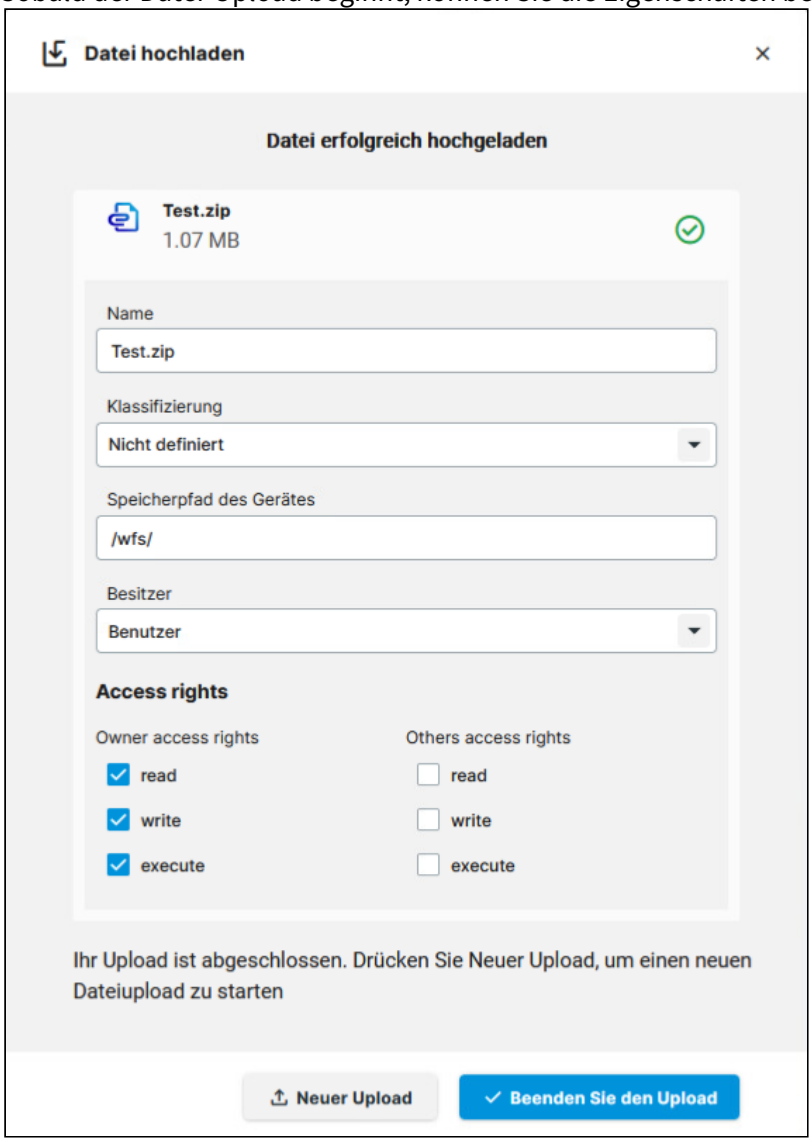
1. Wählen Sie einen Ordner unter Dateien aus. Die Datei wird dorthin hochgeladen.
2. Klicken Sie auf die Schaltfläche **Datei hochladen**.



3. Durchsuchen Sie die Datei oder ziehen Sie sie per Drag&Drop.

> Sie können immer nur eine Datei auf einmal hochladen.

4. Sobald der Datei-Upload beginnt, können Sie die Eigenschaften bearbeiten.



5. Wählen Sie unter **Klassifizierung** die Art der Datei aus. Dies dient dazu, automatisch geeignete Speicherorte und Dateiberechtigungen festzulegen. Wählen Sie zwischen:
   - **Undefiniert**
   - **Webbrowser-Zertifikat**
   - **SSL-Zertifikat**
   - **Java-Zertifikat**
   - **IBM iAccess-Zertifikat**
   - **App Signing Zertifikat**
   - **Allgemeines Zertifikat**

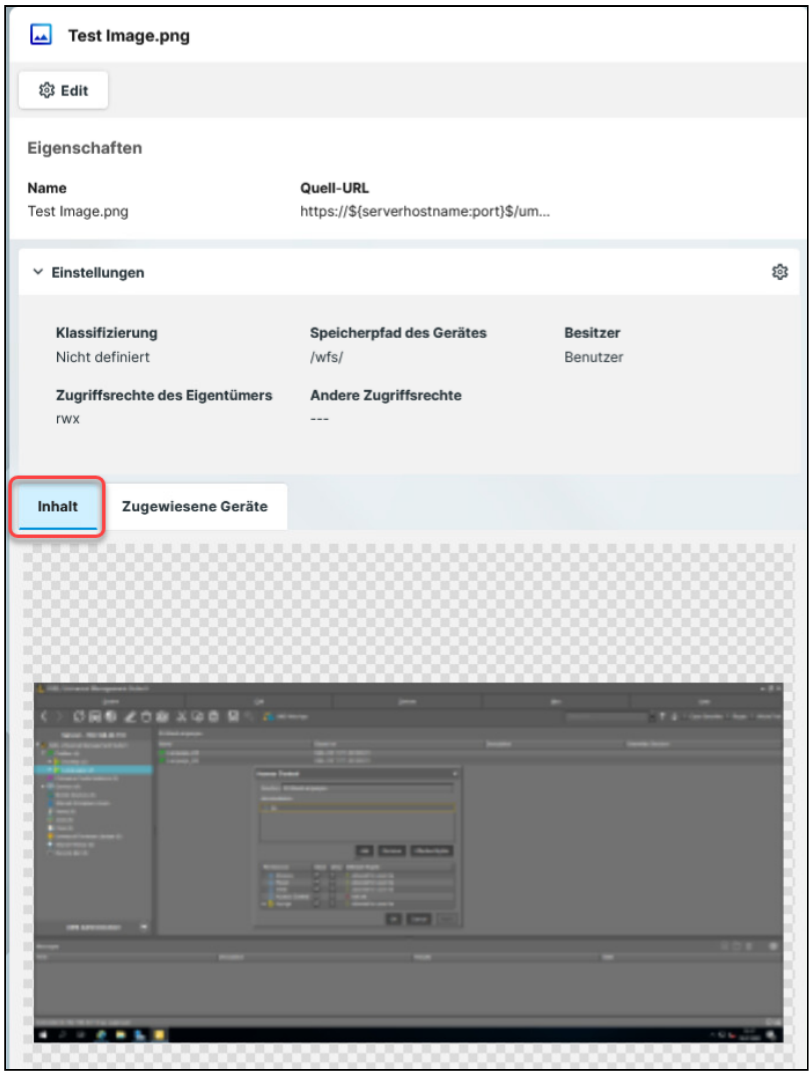
   Informationen zum Einsatz von Zertifikaten finden Sie im Abschnitt "Zertifikate über die UMS bereitstellen" unter Vertrauenswürdige Stammzertifikate in IGEL OS einspielen.

6. Wenn Sie die Klassifizierung auf **Undefiniert** setzen, geben Sie den Pfad im lokalen Dateisystem des Geräts unter **Speicherpfad des Gerätes** an.
   Pfade müssen mit einem Pfadseparator enden - einem Schrägstrich "/" oder einem Backslash "\". Wenn Sie ein Verzeichnis angeben, das noch nicht existiert, wird es automatisch erstellt.

   > Aufgrund der begrenzten Speicherkapazität wird die Verwendung des Ordners `/wfs/` für große Dateien (>2 MB) NICHT empfohlen.

7. Legen Sie für die Klassifizierung **Undefiniert** den **Besitzer** und die **Zugriffsrechte** fest.
   Diese werden an die Datei angehängt, wenn sie auf das Gerät übertragen wird, und werden auf dem Zielsystem verwendet.

8. Klicken Sie auf **Beenden Sie den Upload**, um die Einstellungen zu bestätigen und das Dialogfeld zu schließen, oder auf **Neuer Upload**, um eine andere Datei hochzuladen.
   Sobald der Upload abgeschlossen ist, können Sie auf der Registerkarte **Inhalt** eine Vorschau der hochgeladenen Datei anzeigen. Eine Vorschau wird nur für Dateien angezeigt, die über die IGEL UMS Web App hochgeladen werden.



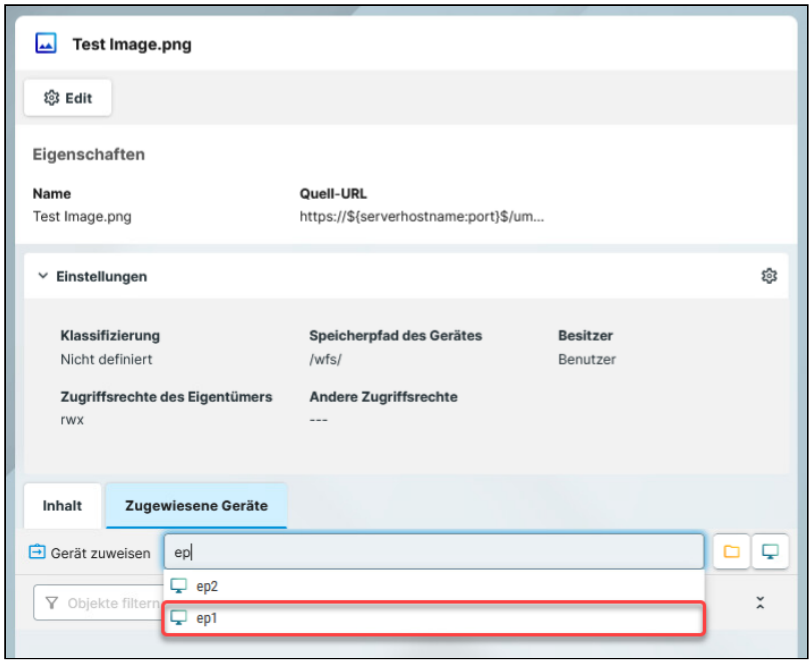
Hochgeladene Dateien können sowohl in der IGEL UMS Web App als auch in der UMS-Konsole verwaltet werden. Einzelheiten zur Verwaltung von Dateien in der UMS-Konsole finden Sie unter Dateien - Dateien am IGEL UMS Server registrieren und zu Geräten übertragen (see page 529).

Dateizuordnung

Im Bereich **Konfiguration** können Sie auf der Registerkarte **Zugewiesene Geräte** einzelne Dateien schnell zuweisen.

1. Wählen Sie die Datei aus, die Sie zuordnen möchten.
2. Wechseln Sie im Informationsdialog auf die Registerkarte **Zugewiesene Geräte**.

3. Geben Sie den Namen des Geräts oder des Geräteverzeichnisses ein.



4. Klicken Sie in der angezeigten Liste auf das Gerät oder Geräteverzeichnis, um die Datei zuzuordnen.

5. Bestätigen Sie die Zuordnung.

Sie können Dateien auch wie alle anderen Objekte über den Bereich **Geräte** zuweisen. Weitere Informationen zur Objektzuweisung finden Sie unter Objekte in der IGEL UMS Web App zuweisen (see page 815)

How to Use Template Keys in Profiles in IGEL Web App

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

Prüfen welche Profile die Parameter in der IGEL UMS Web App definieren

Sie können Profile verwenden, um Geräteparameter in der IGEL Universal Management Suite (UMS) Web App zu definieren. Sie können die durch Profile definierten Parameter für ein bestimmtes Gerät im Gerätekonfigurator überprüfen.

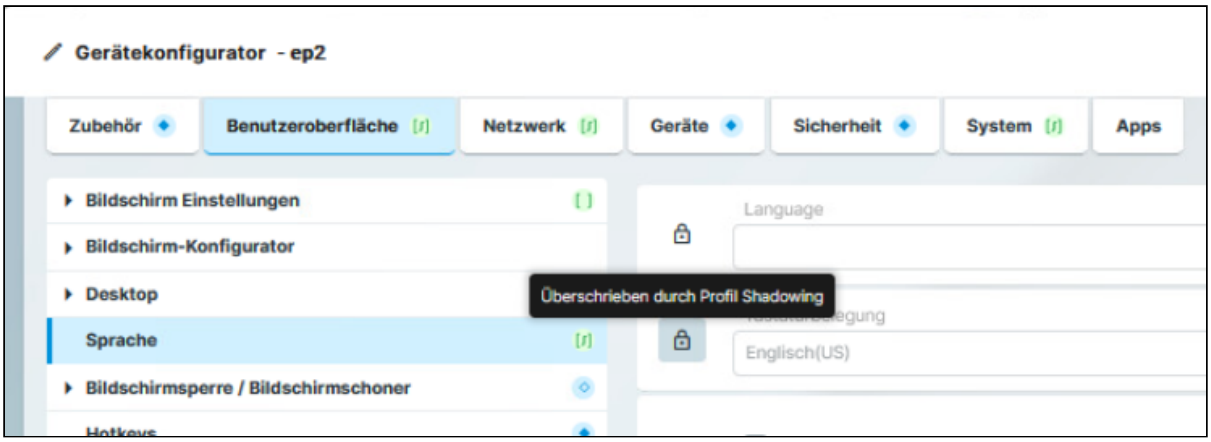
Informationen dazu, wie Sie dies in der UMS-Konsole tun können, finden Sie unter Profile in der IGEL UMS überprüfen (see page 382).

Sie können dies wie folgt überprüfen:

1. Gehen Sie in der UMS Web App zu Geräte und wählen Sie das gewünschte Gerät aus.

2. Klicken Sie in den **Gerätebefehlen auf [Kontextmenü des Geräts] > Konfiguration bearbeiten** oder **Konfiguration bearbeiten**. Oder Sie doppelklicken einfach auf das Gerät.
   Der Gerätekonfigurator öffnet sich und zeigt die aktuelle Konfiguration für das Gerät an. Vor jeder Einstellung, die über ein zugewiesenes Profil konfiguriert wurde, wird ein Schlosssymbol angezeigt. Der Wert, den Sie im Profil angegeben haben, wird angezeigt.

3. Fahren Sie mit der Maus über das Schlosssymbol.
   In einem Tooltip wird angezeigt, aus welchem Profil der Parameterwert übernommen wurde. Dies ist nützlich, wenn Sie dem Gerät mehr als ein Profil zugewiesen haben.



Wenn eine Einstellung in mehreren zugewiesenen Profilen aktiv ist, gilt der Wert nach der Priorisierung, die in Prioritization of Profiles in the IGEL UMS beschrieben ist.

Apps - Import und Konfiguration von Apps für IGEL OS 12-Geräte über die UMS Web App

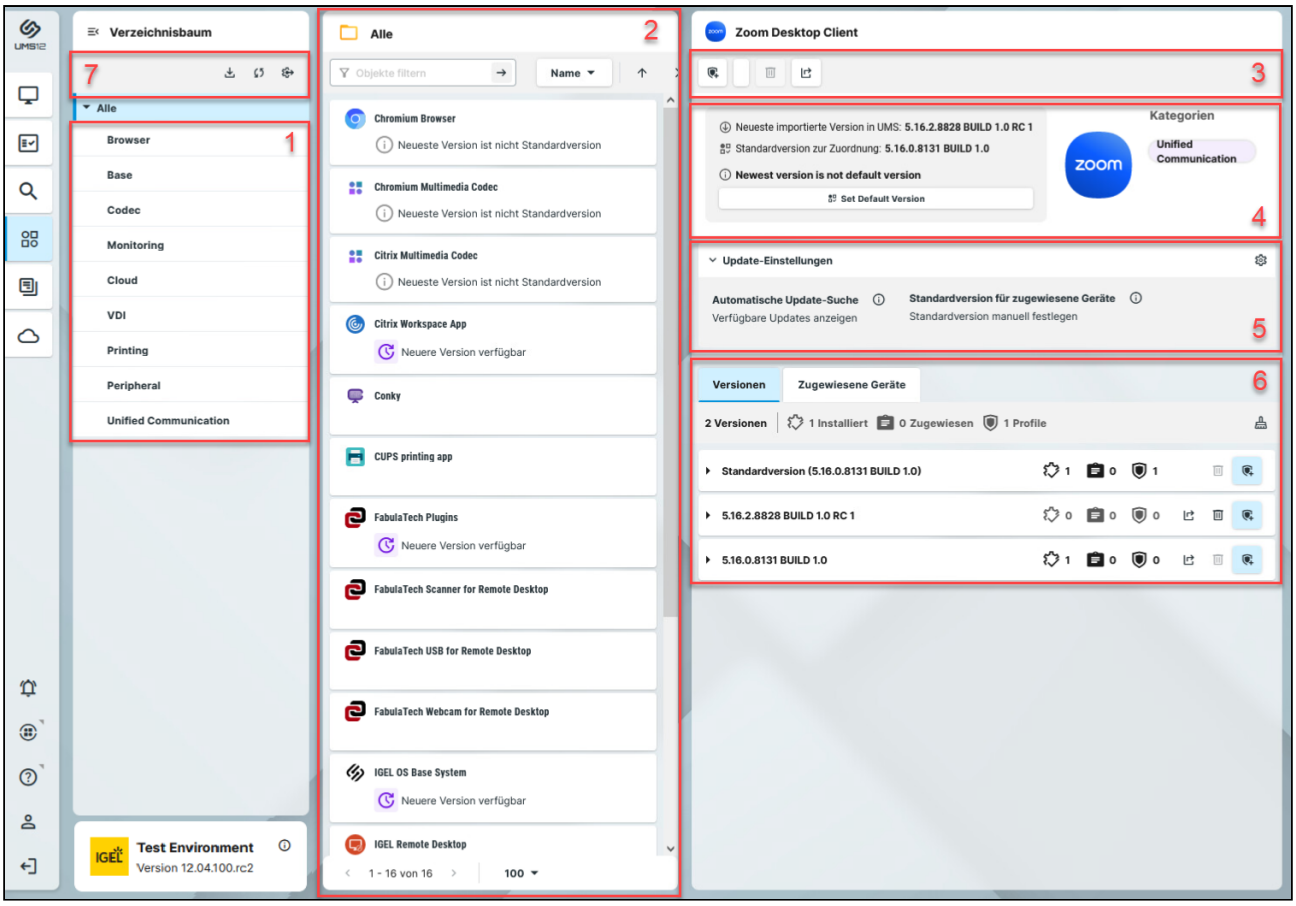
Im Bereich **Apps** der UMS Web App können Sie Apps verwalten, die Sie zur Konfiguration Ihrer IGEL OS 12-Geräte in die IGEL Universal Management Suite (UMS) importieren.

> Für den Zugriff auf den Bereich **Apps** benötigen Sie die Berechtigung **App Management**. Sie können die Berechtigung in der **UMS Konsole > System > Administratorkonten** setzen.
> Allgemeine Informationen zu Rechten finden Sie unter Administratorkonten und Zugriffsrechte (see page 676).

Menüpfad: **UMS Web App > Apps**

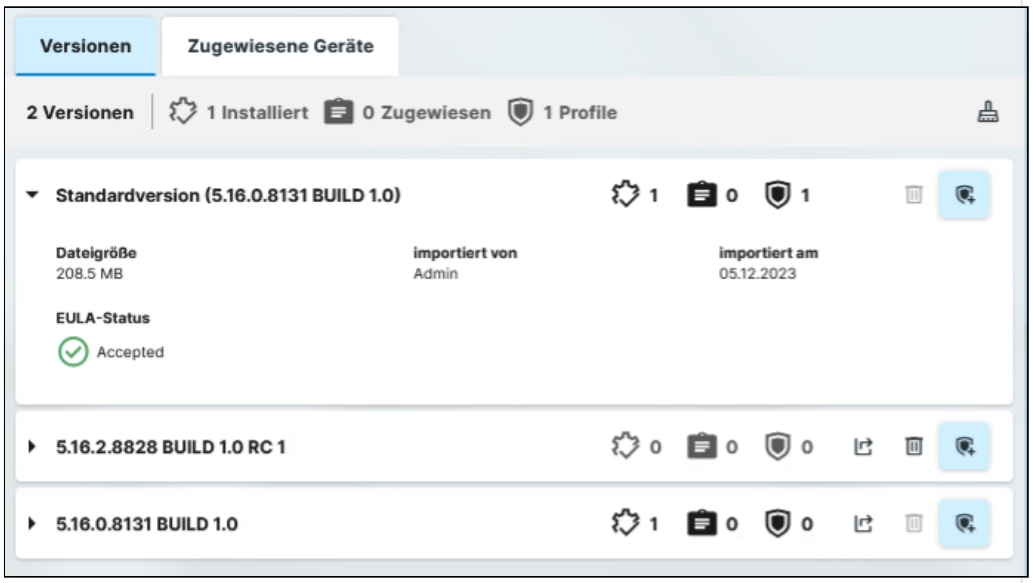
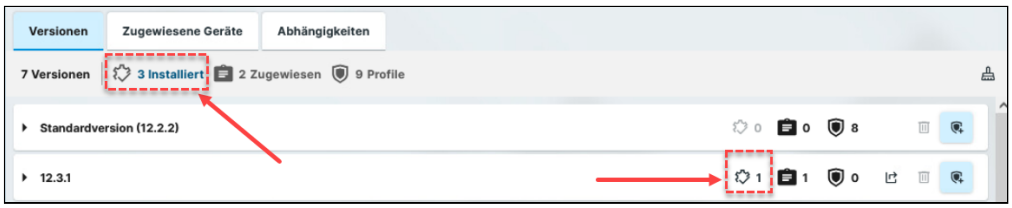
Unter **Apps** finden Sie

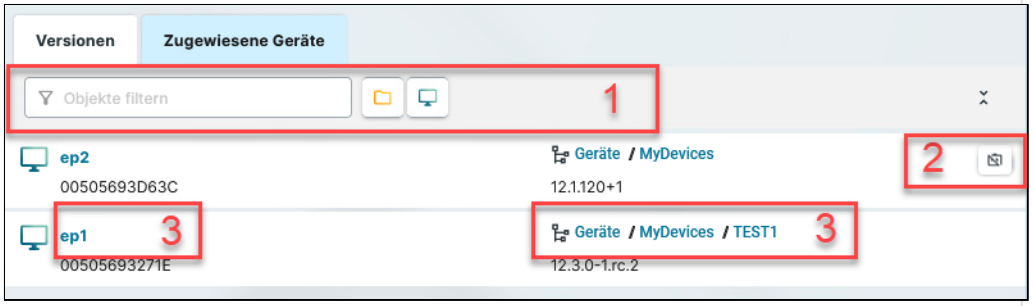
- Apps, die vom IGEL App Portal importiert wurden
- automatisch registrierte Apps. Die UMS registriert automatisch alle auf den Geräten verfügbaren Apps, z. B. IGEL OS Base System, lokal installierte Apps und abhängige Apps, die bei der Installation der Haupt-App automatisch auf dem Gerät installiert werden (z. B. Citrix Multimedia Codec als abhängige App für Citrix Workspace App).



1	App-Kategorien	Zeigt alle verfügbaren App-Kategorien an. ▶ Klicken Sie **Alle**, um Apps aus allen Kategorien anzuzeigen. ▶ Klicken Sie auf eine bestimmte Kategorie, um alle Apps innerhalb dieser Kategorie anzuzeigen.
2	App-Liste	Zeigt die in der ausgewählten Kategorie enthaltenen Apps an. • Paging für die Navigation in der App-Liste • Anzahl der auf einer Seite anzuzeigenden Apps definieren • Apps nach **Namen** filtern • Apps nach **Namen** sortieren

3	Befehle	**Neues Profil anlegen**: Erstellt ein Profil für die in der App-Liste ausgewählte App. Weitere Informationen zur Profilerstellung finden Sie unter Profile in der IGEL UMS Web App erstellen und zuweisen (see page 838). **Standardversion festlegen**: Legt fest, welche App-Version einem Gerät / Geräteverzeichnis zugewiesen wird, wenn keine bestimmte App-Version bei der App-Zuweisung oder bei der Erstellung eines Profils, das diese App konfiguriert, ausgewählt wird. Siehe Standardversion einer App in der IGEL UMS festlegen (see page 876). **App löschen**: Löscht eine in der App-Liste ausgewählte App, wenn diese App nirgendwo verwendet wird. Siehe Apps in der IGEL UMS Web App löschen (see page 886). **App exportieren (Metadaten)**: Exportiert die Metadaten einer in der App-Liste ausgewählten App, siehe Export und Hochladen von Apps in der IGEL UMS (see page 894).
4	App-Informationen	Details zu der in der App-Liste ausgewählten App, z. B. **Neueste importierte Version**, **Standardversion**, die unter **Standardversion festlegen** ausgewählt ist, Verfügbarkeit einer neueren Version (je nach Konfiguration unter **Update-Einstellungen**).
5	Update-Einstellungen	Legt die Update-Einstellungen für die in der App-Liste ausgewählte App fest. Siehe Configuring Update Settings for Individual IGEL OS Apps (see page 890).

6	Versionen	Zeigt Informationen zu allen verfügbaren Versionen einer App an, z.B. ob und wie eine App-Version verwendet wird (installiert, zugewiesen, in Profilen verwendet).  ▶ Um die ausgewählte App-Version zu exportieren, klicken Sie auf . ▶ Um eine ausgewählte App-Version zu löschen, klicken Sie . Siehe Apps in der IGEL UMS Web App löschen (see page 886). ▶ Um ein Profil aus der ausgewählten App-Version zu erstellen, klicken Sie auf . Einzelheiten zu Profilen finden Sie unter Profile in der IGEL UMS Web App erstellen und zuweisen (see page 838).  ▶ Um die Liste der Geräte anzuzeigen, auf denen eine beliebige Version der App installiert ist, klicken Sie auf den Link am oberen Rand der Registerkarte. Die Liste wird in einer neuen Registerkarte als Suche geöffnet.

	▶ Um die Liste der Geräte anzuzeigen, auf denen die ausgewählte Version der App installiert ist, klicken Sie auf die Schaltfläche in der Zeile mit der App-Version. Die Liste wird in einer neuen Registerkarte als Suche geöffnet. Eine App-Version, für die der Endbenutzer-Lizenzvertrag (End User License Agreement, EULA) nicht akzeptiert wurde, ist mit einem Ausrufezeichen gekennzeichnet. ▶ Um die EULA für die App zu akzeptieren, klicken Sie **EULA akzeptieren**. Dies kann z. B. bei automatisch registrierten Apps (see page 862) notwendig sein oder wenn die EULA geändert wird. Wenn die EULA in der UMS nicht akzeptiert wird, kann sie dennoch von Ihren Benutzern lokal auf dem Gerät über den entsprechenden Benachrichtigungsdialog akzeptiert werden.
Zugewiesene Geräte	Zeigt alle Geräte / Geräteverzeichnisse an, denen die ausgewählte App zugewiesen ist.  1: Filtert die Geräte / Geräteverzeichnisse, die der ausgewählten App zugeordnet sind. Die Filterkriterien werden mit dem Operator *AND* verknüpft. ▶ Klicken Sie , um alle Filter zu entfernen. 2: Entfernt das ausgewählte Gerät / Geräteverzeichnis von der App. 3: Springt zu dem entsprechenden Gerät / Verzeichnis und zeigt alle **Zugewiesenen Objekte** dafür an.

Abhängigkeiten	Zeigt Informationen darüber an, wie sich die ausgewählte App-Version zu anderen Apps verhält.

1: Versionsselektor

▶ Wählen Sie aus der Dropdown-Liste die Version aus, für die Sie die Abhängigkeitsinformationen sehen möchten.

2: Informationen über Abhängigkeiten

▶ Klicken Sie auf das Tooltip-Symbol, um die detaillierte Beschreibung zu erhalten:

- **Erforderliche Apps**

Die vorliegende App-Version benötigt andere Apps, um voll funktionsfähig zu sein.

Wenn eine erforderliche App nur als Name erwähnt wird, ist jede Version dieser App ausreichend.
Wenn eine bestimmte Version erwähnt wird, wird die erforderliche App in exakt dieser Version benötigt.
Wenn ein Minimalwert angegeben ist, muss die App in einer neueren Version vorliegen.
Wenn ein Maximalwert angegeben ist, muss die App in einer älteren Version vorliegen.

Falls der Administrator nicht aktiv eine Version der benötigten App zuweist, wird das Gerät versuchen, diese selbst zu berechnen und zu installieren.

		• **Mögliche Konflikte** Die vorliegende App-Version kann nicht gleichzeitig mit den hier aufgelisteten Apps installiert werden. Wenn eine App nur als Name aufgelistet ist, darf keine Version dieser App installiert sein. Wenn eine bestimmte Version erwähnt wird, ist nur diese Version ausgeschlossen. Wenn ein Maximalwert angegeben ist, kann die App nicht in einer Version unterhalb dieses Werts installiert sein. Wenn ein Minimalwert angegeben ist, kann die App nicht in einer Version oberhalb dieses Werts installiert sein.
7	Einstellungen	Ermöglicht die Konfiguration globaler Einstellungen für die App-Updates. Siehe Configuring Global Settings for the Update of IGEL OS Apps (see page 889).

- IGEL OS Apps vom IGEL App Portal importieren (see page 869)
- Installation von OS 12-Apps in einer UMS Umgebung mit begrenztem oder keinem Internetzugang (see page 872)
- Standardversion einer App in der IGEL UMS festlegen (see page 876)
- Apps zu IGEL OS Geräten über die UMS Web App zuweisen (see page 878)
- Checking Installed Apps via the IGEL UMS Web App (see page 882)
- Apps vom IGEL OS-Gerät entfernen in IGEL UMS Web App (see page 883)
- Apps in der IGEL UMS Web App löschen (see page 886)
- Updating IGEL OS Apps (see page 888)
- Export und Hochladen von Apps in der IGEL UMS (see page 894)

IGEL OS Apps vom IGEL App Portal importieren

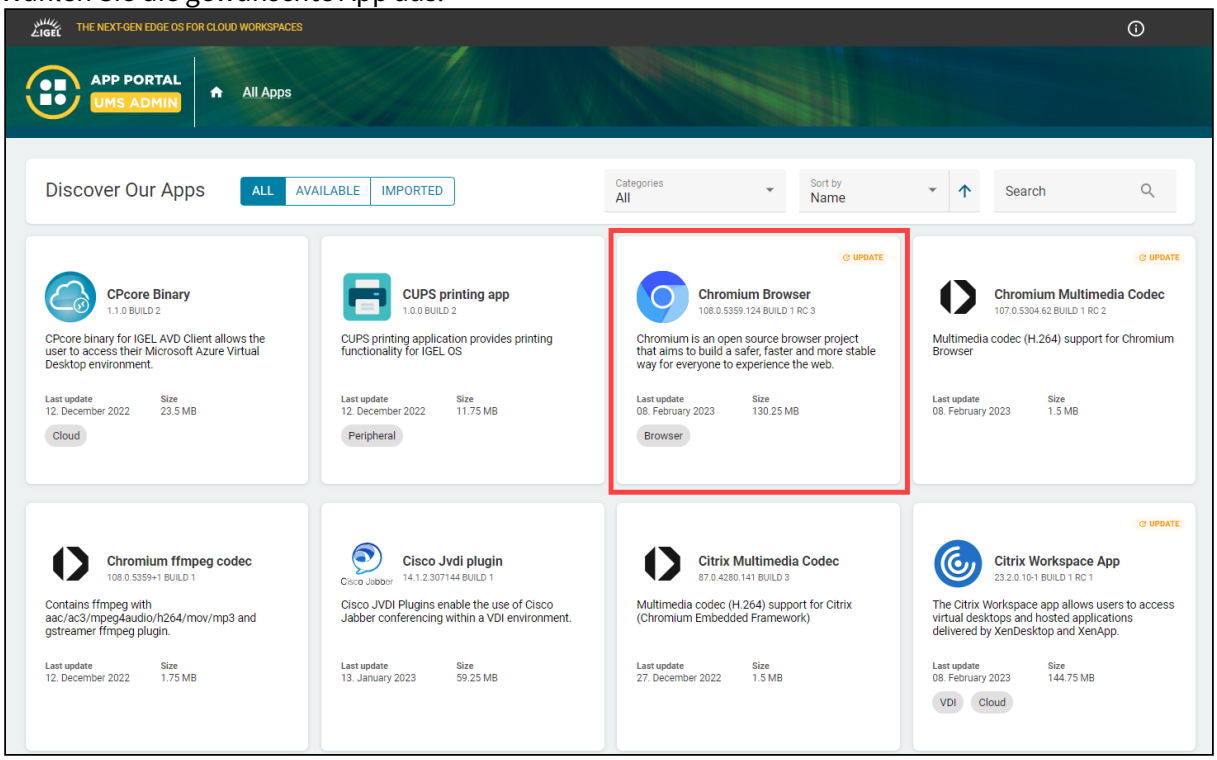
Um IGEL OS 12 Geräte zu verwalten, müssen Sie IGEL OS Apps Ihrer Wahl von dem IGEL App Portal importieren.

> Um auf das IGEL App Portal zugreifen zu können, müssen Sie zunächst Ihre IGEL Universal Management Suite (UMS) registrieren; siehe Registrierung der IGEL Universal Management Suite (UMS).

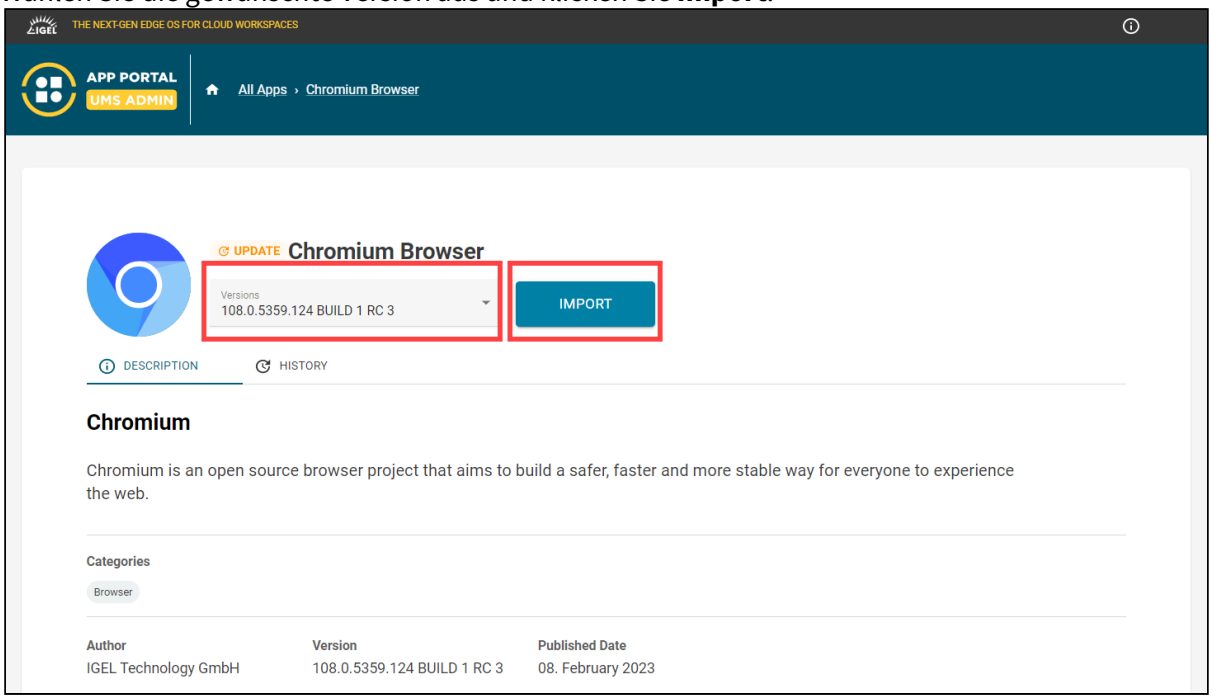
So importieren Sie Apps in die IGEL UMS:

1. Klicken Sie in der UMS Web App auf **App Portal**.

2. Wählen Sie die gewünschte App aus.

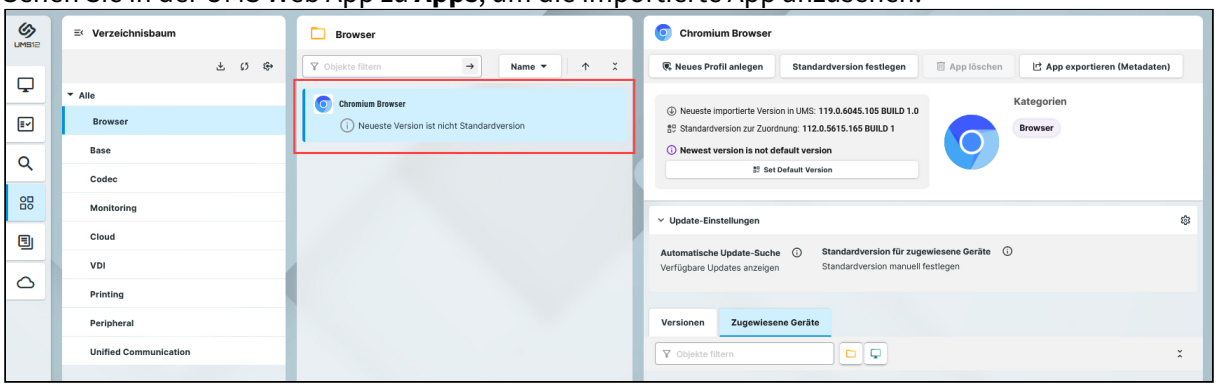


3. Wählen Sie die gewünschte Version aus und klicken Sie **Import**.



4. Akzeptieren Sie End User License Agreement (EULA) und warten Sie, bis das Importieren abgeschlossen ist.

5. Gehen Sie in der UMS Web App zu **Apps**, um die importierte App anzusehen.



Installation von OS 12-Apps in einer UMS Umgebung mit begrenztem oder keinem Internetzugang

Wenn Ihre IGEL Universal Management Suite (UMS) ohne Internetverbindung läuft und Sie sie zur Installation von Apps auf IGEL OS 12 Geräten verwenden möchten, können Sie die Apps vor der App-Zuweisung manuell in die UMS Web App hochladen. Wenn Ihre OS 12 Geräte ebenfalls ohne Internetverbindung laufen, müssen Sie Ihre UMS vor der App-Zuweisung auch als Update-Proxy konfigurieren.

> Ein zusätzlicher FTP-Server ist in keinem Fall erforderlich, da alles von der IGEL UMS und den IGEL OS Geräten erledigt wird.

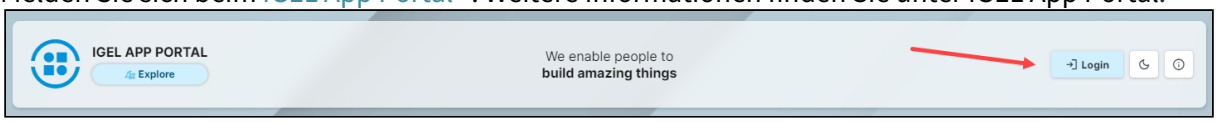
Direkter Zugriff auf das IGEL App Portal

Sie müssen auf das App Portal zugreifen, um die App-Pakete für den manuellen Upload herunterzuladen. Da das UMS keinen Internetzugang hat, können Sie nicht über die UMS Web App auf das App Portal zugreifen. Stattdessen müssen Sie auf das App Portal zugreifen, indem Sie sich direkt dort anmelden. Weitere Informationen finden Sie unter IGEL App Portal.

UMS ohne Internetzugang aber OS 12 Geräte mit Internetzugang

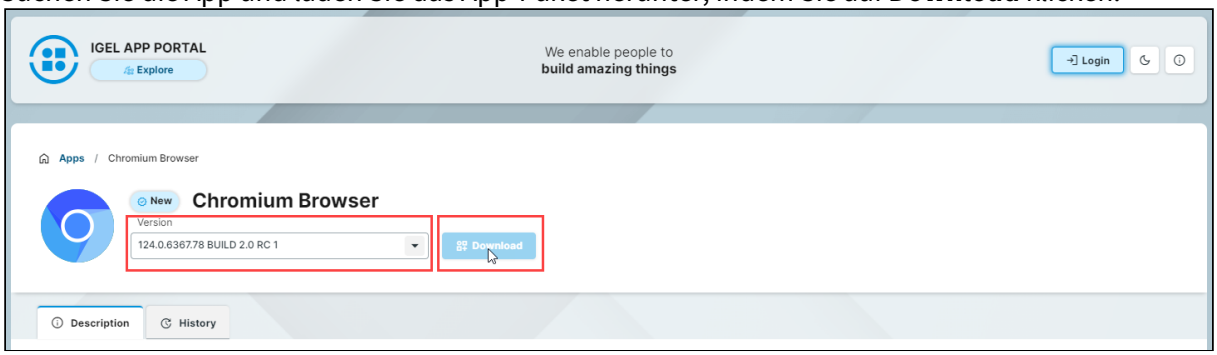
Wenn die UMS nicht mit dem Internet verbunden ist, die OS 12 Geräte aber schon, müssen Sie die Apps manuell auf die UMS hochladen, anstatt sie aus dem IGEL App Portal zu importieren. Dann werden die Apps über die UMS zugewiesen, und die Geräte erhalten die App-Binärdateien aus dem IGEL App Portal. So installieren Sie Apps auf OS 12 Geräten:

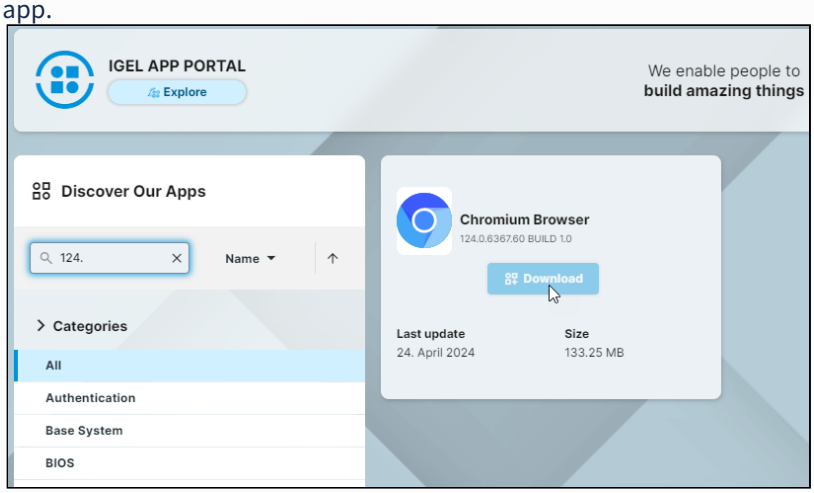
1. Melden Sie sich beim IGEL App Portal[38]. Weitere Informationen finden Sie unter IGEL App Portal.



38 https://app.igel.com/

2. Suchen Sie die App und laden Sie das App-Paket herunter, indem Sie auf **Download** klicken.



> If you click the **Download** action button in the cards view, you download the latest version of the app.
>
> 
>

3. Laden Sie das heruntergeladene App-Paket in die UMS Web App hoch. Weitere Informationen finden Sie im Abschnitt Apps Hochladen unter Export und Hochladen von Apps in der IGEL UMS (see page 894).

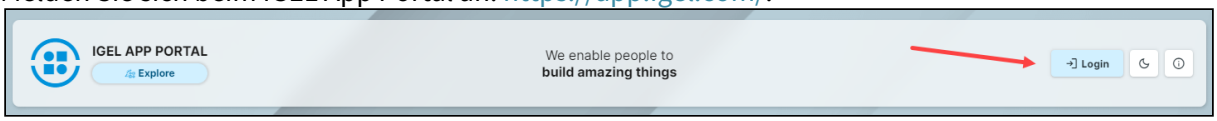
4. Weisen Sie die App den Geräten zu. Detaillierte Anweisungen finden Sie unter Apps zu IGEL OS Geräten über die UMS Web App zuweisen (see page 878).

   Die Geräte erhalten die App-Binärdateien über das App-Portal.

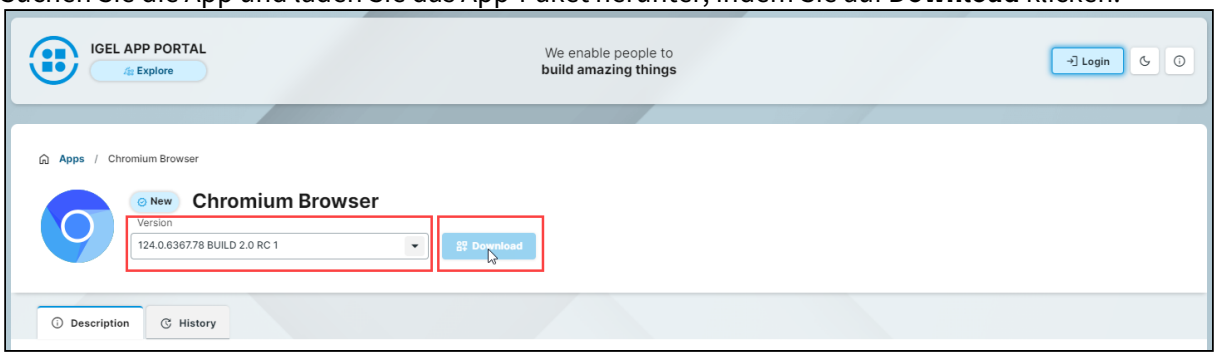
UMS und OS 12 Devices ohne Internetzugang

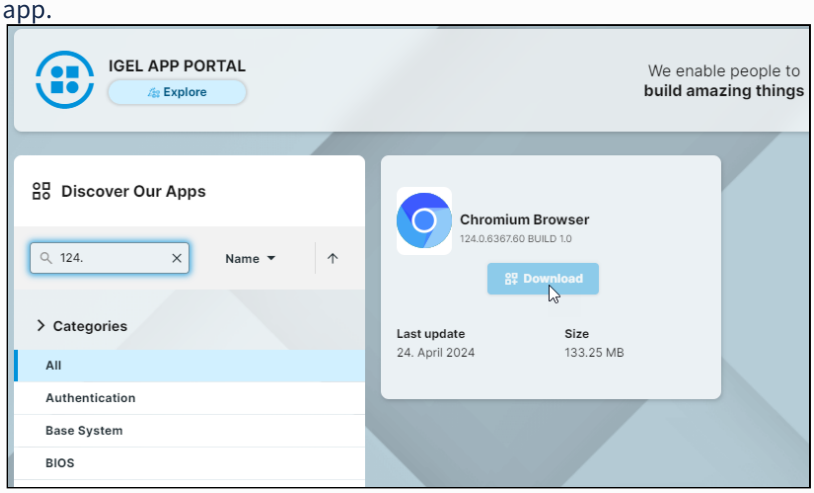
Wenn sowohl die UMS als auch die OS 12 Geräte nicht mit dem Internet verbunden sind, müssen Sie Ihre UMS als Update-Proxy konfigurieren. Dadurch können die Geräte die App-Binärdateien direkt von der UMS beziehen. So installieren Sie Apps auf OS 12 Geräten:

1. Melden Sie sich beim IGEL App Portal an: https://app.igel.com/.



2. Suchen Sie die App und laden Sie das App-Paket herunter, indem Sie auf **Download** klicken.



> If you click the **Download** action button in the cards view, you download the latest version of the app.
>
> 
>

3. Legen Sie die UMS als Update-Proxy fest, indem Sie unter **UMS Web App > Apps > Einstellungen**  **> UMS als Update-Proxy** die Option **Von UMS herunterladen** wählen. Weitere Informationen finden Sie im Abschnitt UMS as an Update Proxy unter Configuring Global Settings for the Update of IGEL OS Apps (see page 889).

4. Laden Sie das App-Paket hoch. Weitere Informationen finden Sie im Abschnitt Apps Hochladen unter Export und Hochladen von Apps in der IGEL UMS (see page 894).

> ⚠ Laden Sie die Datei im `.ipkg` Format hoch, da so sichergestellt wird, dass die Binärdateien korrekt in das UMS hochgeladen werden.

5. Weisen Sie die App den Geräten zu. Detaillierte Anweisungen finden Sie unter Apps zu IGEL OS Geräten über die UMS Web App zuweisen (see page 878).
   Die Geräte erhalten App-Binärdateien direkt von der UMS.

Standardversion einer App in der IGEL UMS festlegen

Wenn Sie mehrere Versionen einer App in die IGEL Universal Management Suite (UMS) importieren, können Sie festlegen, welche Version als **Standardversion** fungieren soll.

Die **Standardversion** ist eine Version, die einem Gerät/Geräteverzeichnis zugewiesen wird, wenn bei der Zuweisung einer App (siehe Apps zu IGEL OS Geräten über die UMS Web App zuweisen (see page 878)) oder bei der Erstellung eines Profils, das diese App konfiguriert (siehe Profile in der IGEL UMS Web App erstellen und zuweisen (see page 838)) keine Version angegeben wird.

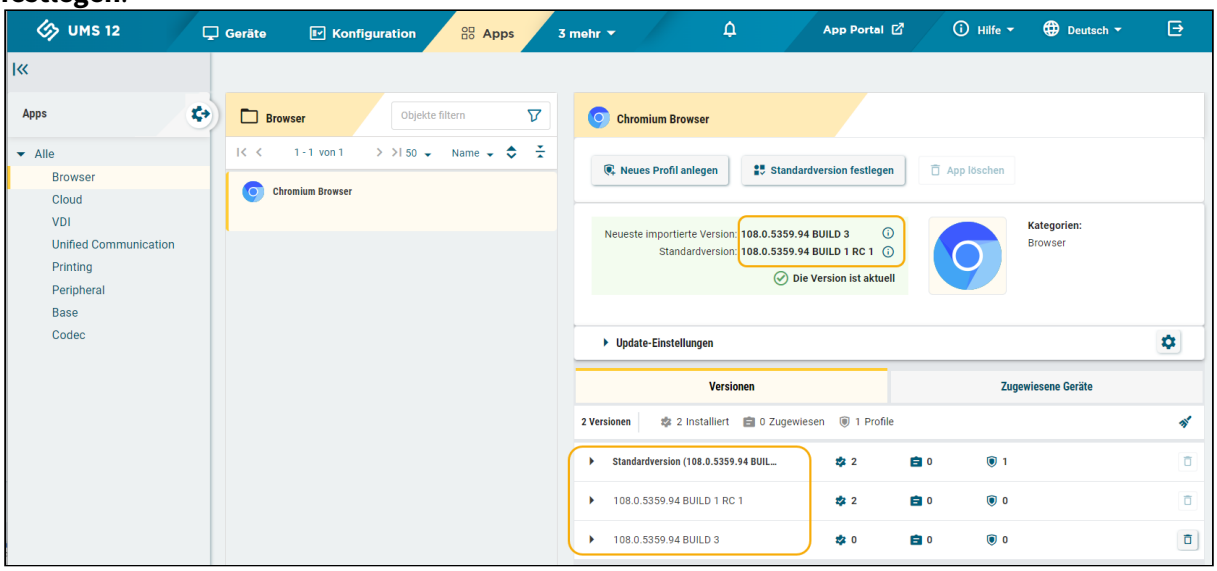
Eine **Standardversion** wird global festgelegt: Wenn sie geändert wird, werden alle Zuweisungen, bei denen keine Version explizit angegeben wurde, mitgeändert.

Die beste Vorgehensweise bei der App-Zuweisung und Profilerstellung ist die Verwendung der **Standardversion**.
Die Verwendung einer bestimmten Version während der App-Zuweisung und Profilerstellung wird für Testzwecke empfohlen, z. B. um App-Updates zu testen. Nach erfolgreichen Tests können Sie Ihre Standardversion ändern.

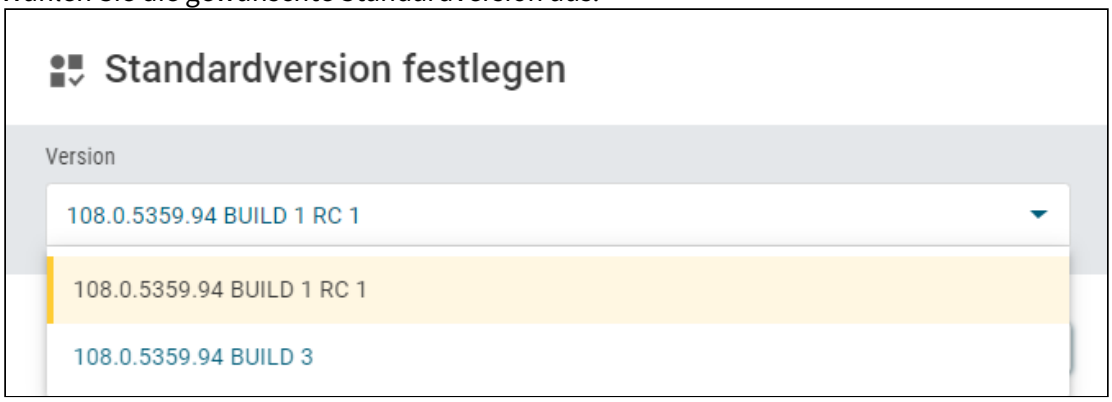
Menüpfad: **UMS Web App > Apps**

So definieren Sie eine Standardversion für eine App:

1. Wählen Sie unter **UMS Web App > Apps** die gewünschte App aus und klicken Sie **Standardversion festlegen**.



2. Wählen Sie die gewünschte Standardversion aus.



3. Speichern Sie die Änderungen.

Apps zu IGEL OS Geräten über die UMS Web App zuweisen

In der IGEL Universal Management Suite (UMS) gibt es zwei Methoden, um Ihren Geräten eine App zuzuweisen:

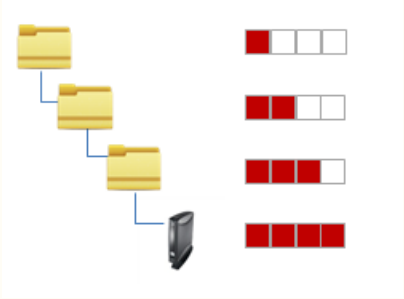
- Implizite App-Zuweisung über Profile: Eine App wird einem Gerät automatisch über ein Profil zugewiesen, das diese App konfiguriert. Ausnahmen: IGEL OS Base System App. Siehe Profile in der IGEL UMS Web App erstellen und zuweisen (see page 838).
- Explizite App-Zuweisung über den Dialog **Objekt zuweisen**, siehe unten.

> Eine explizit zugewiesene App überschreibt eine implizit zugewiesene App.

Explizite App-Zuweisung

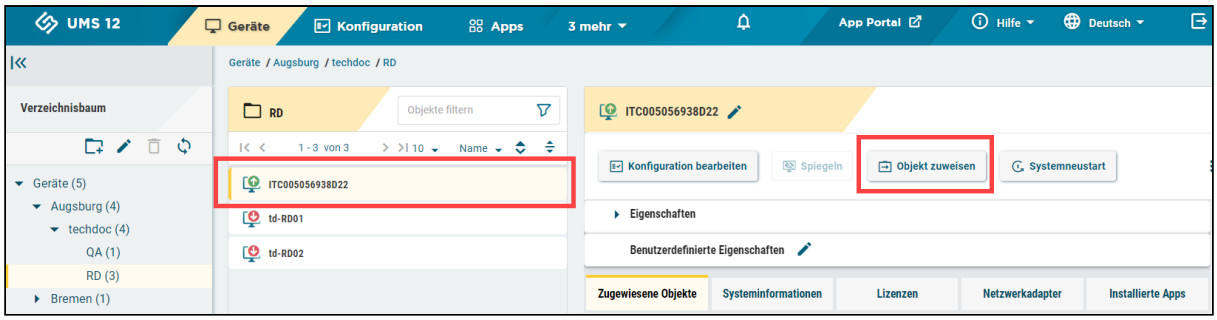
> Für die Zuweisung der IGEL OS Base System App ist die Berechtigung **Basissystem / Firmwareupdate zuordnen** erforderlich. Sie können die Berechtigung in der UMS Konsole über **[Kontextmenü eines Geräts / Geräteverzeichnisses] > Berechtigungen** setzen.
> Allgemeine Informationen zu Berechtigungen finden Sie unter Administratorkonten und Zugriffsrechte (see page 676).

> Sind einem Gerät verschiedene App-Versionen zugewiesen (z.B. über direkte und indirekte Zuweisung), hat die Version, die dem Gerät im Verzeichnisbaum näher ist, Vorrang und wird auf dem Gerät installiert.



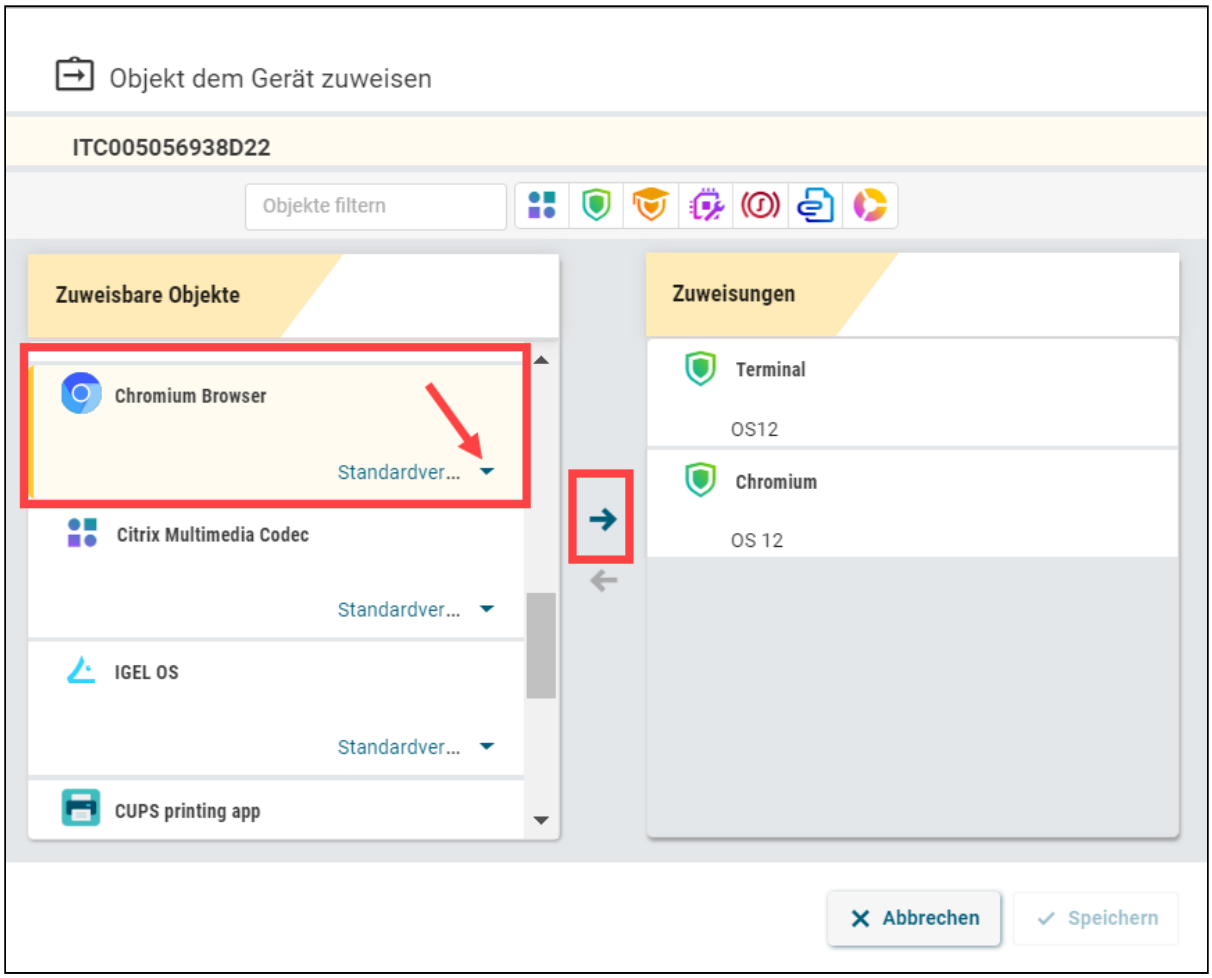
Um Apps einem Gerät / Geräteverzeichnis zuzuweisen, gehen Sie wie folgt vor:

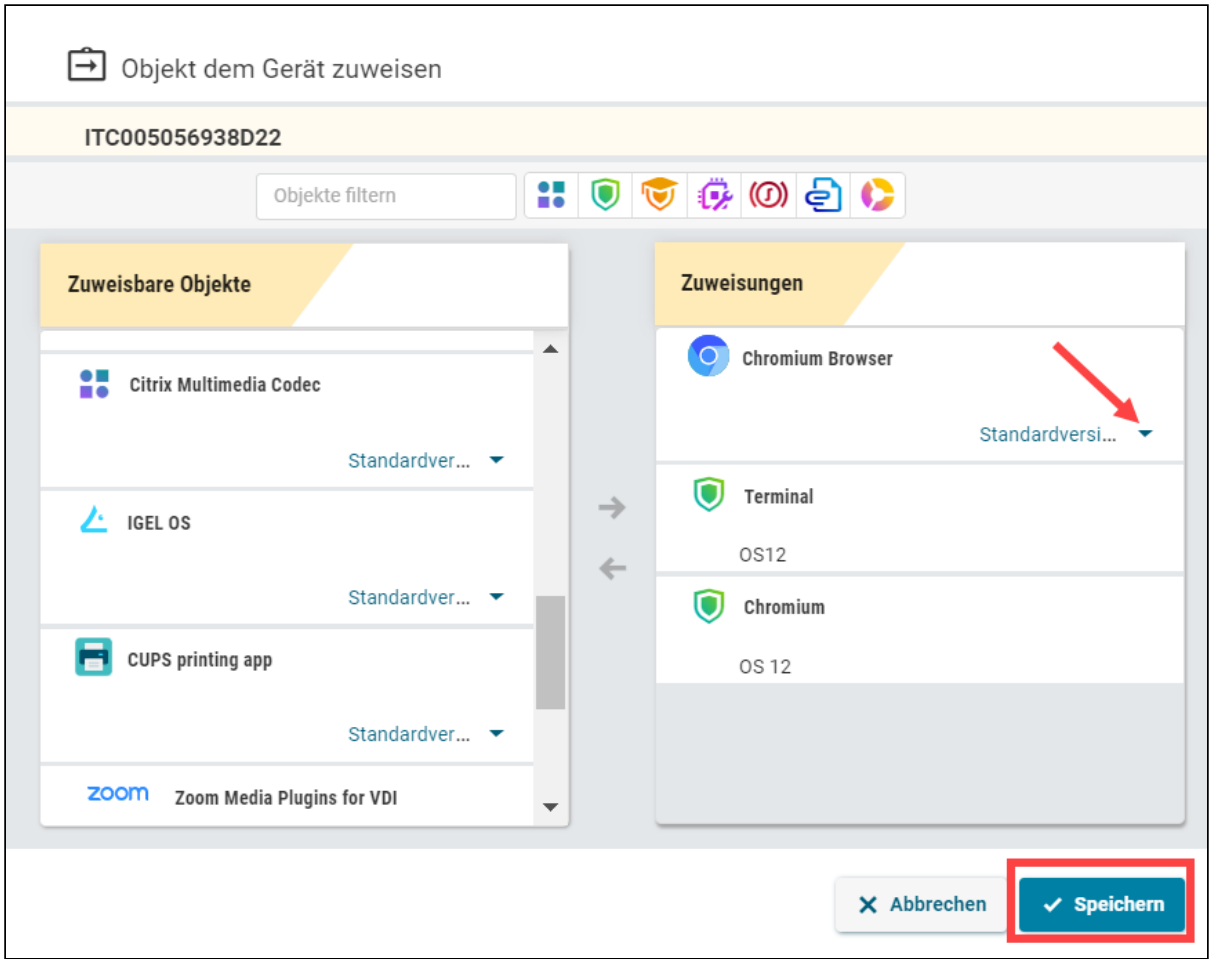
1. Wählen Sie unter **UMS Web App > Geräte** ein Gerät oder Geräteverzeichnis aus und klicken Sie **Objekt zuweisen**.



2. Wählen Sie die gewünschte App (und eine bestimmte Version, falls nötig).

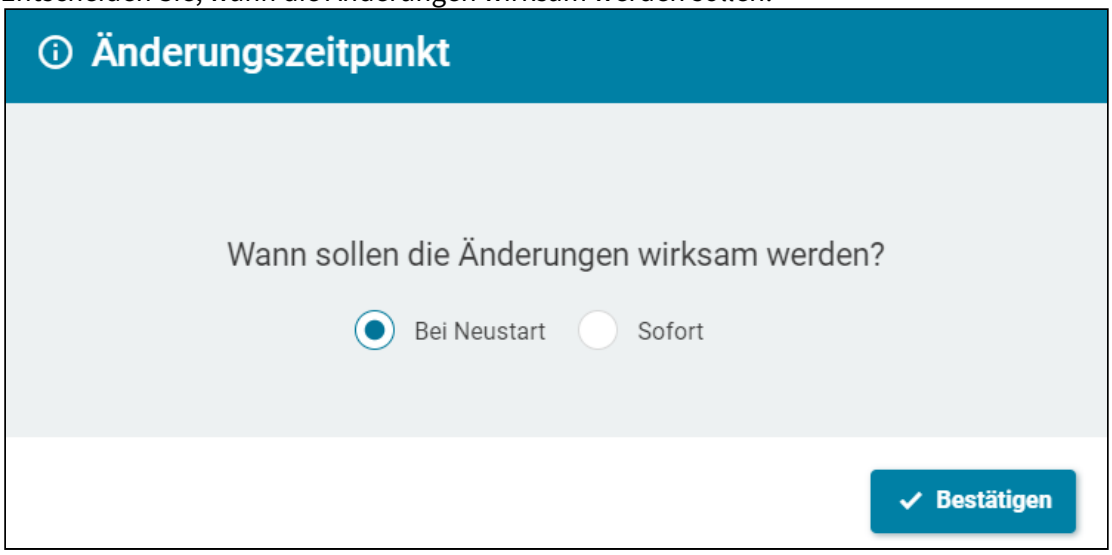
> Wenn bei der Zuweisung keine Version für eine App angegeben wird, wird die Standardversion (see page 876) verwendet. Es ist möglich, die Version für eine App im Dialog **Objekt zuweisen** entweder unter **Zuweisbare Objekte** oder unter **Zuweisungen** auszuwählen.





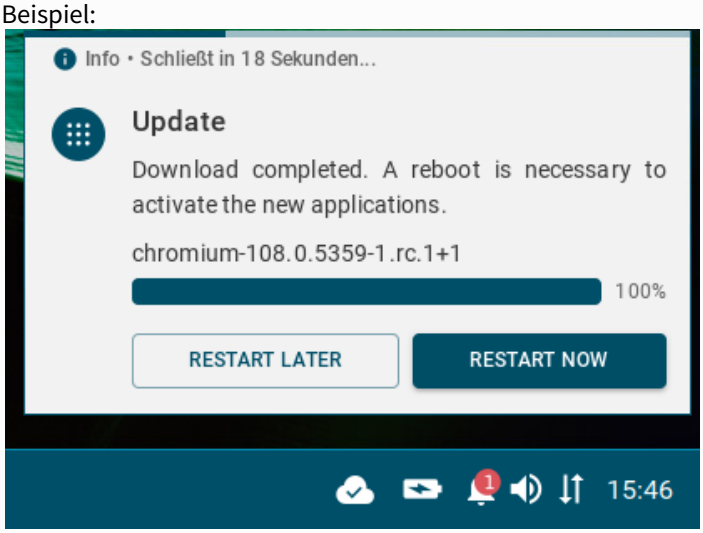
3. Speichern Sie die Änderungen.

4. Entscheiden Sie, wann die Änderungen wirksam werden sollen.



Die App wird auf das Gerät heruntergeladen.

Standardmäßig werden die Apps / App-Versionen beim nächsten Neustart automatisch aktiviert. Der Benutzer erhält eine entsprechende Benachrichtigung.
Beispiel:



Wenn Sie das Background App Update konfiguriert haben, muss stattdessen ein **Update**-Befehl gesendet werden. Weitere Informationen finden Sie unter How to Configure the Background App Update in the IGEL UMS Web App (see page 893).

Die zugewiesene App wird in der UMS Web App unter **Geräte > Zugewiesene Objekte** angezeigt.

Um die installierten Apps zu überprüfen, gehen Sie zu **Geräte > [Name des Geräts] > Installierte Apps**; siehe Checking Installed Apps via the IGEL UMS Web App (see page 882).

Checking Installed Apps via the IGEL UMS Web App

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

Apps vom IGEL OS-Gerät entfernen in IGEL UMS Web App

In der IGEL Universal Management Suite (UMS) Web App können Sie Apps entfernen, die Sie nicht mehr benötigen.

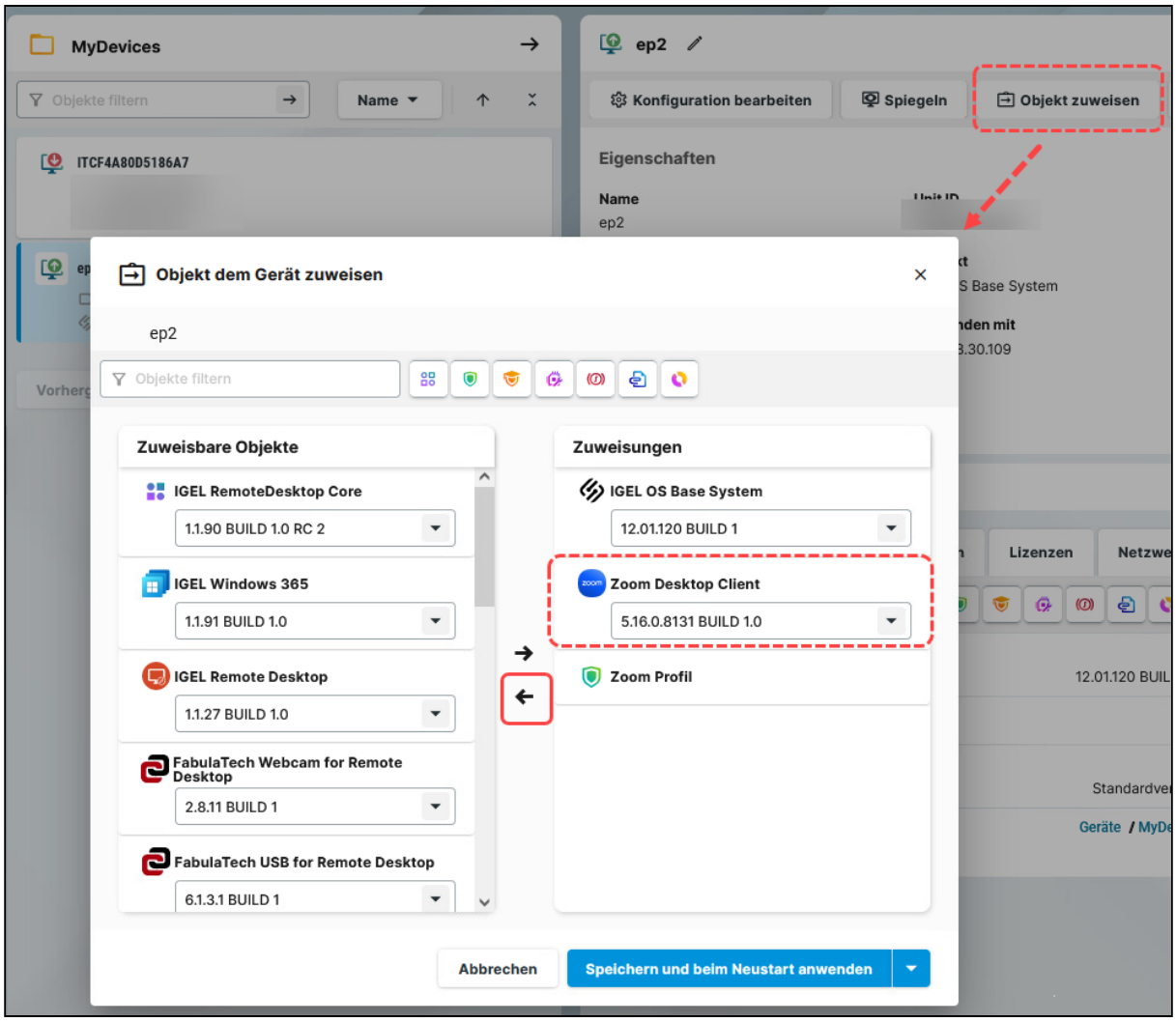
⚠ Im Falle der expliziten App-Zuweisung: Wenn Sie eine App von einem Gerät entfernen, wird diese App **auf dem Gerät deinstalliert**. Ausnahme: Die IGEL OS Base System App ist nicht deinstallierbar.
Im Falle der impliziten App-Zuweisung: Wenn Sie ein Profil von einem Gerät entfernen, wird die über dieses Profil konfigurierte App **auf dem Gerät deinstalliert**.
Weitere Informationen zur impliziten und expliziten App-Zuweisung finden Sie unter Apps zu IGEL OS Geräten über die UMS Web App zuweisen (see page 878).

Menüpfad: **UMS Web App > Geräte > [Name des Geräts / Geräteverzeichnisses] > Objekt zuweisen**

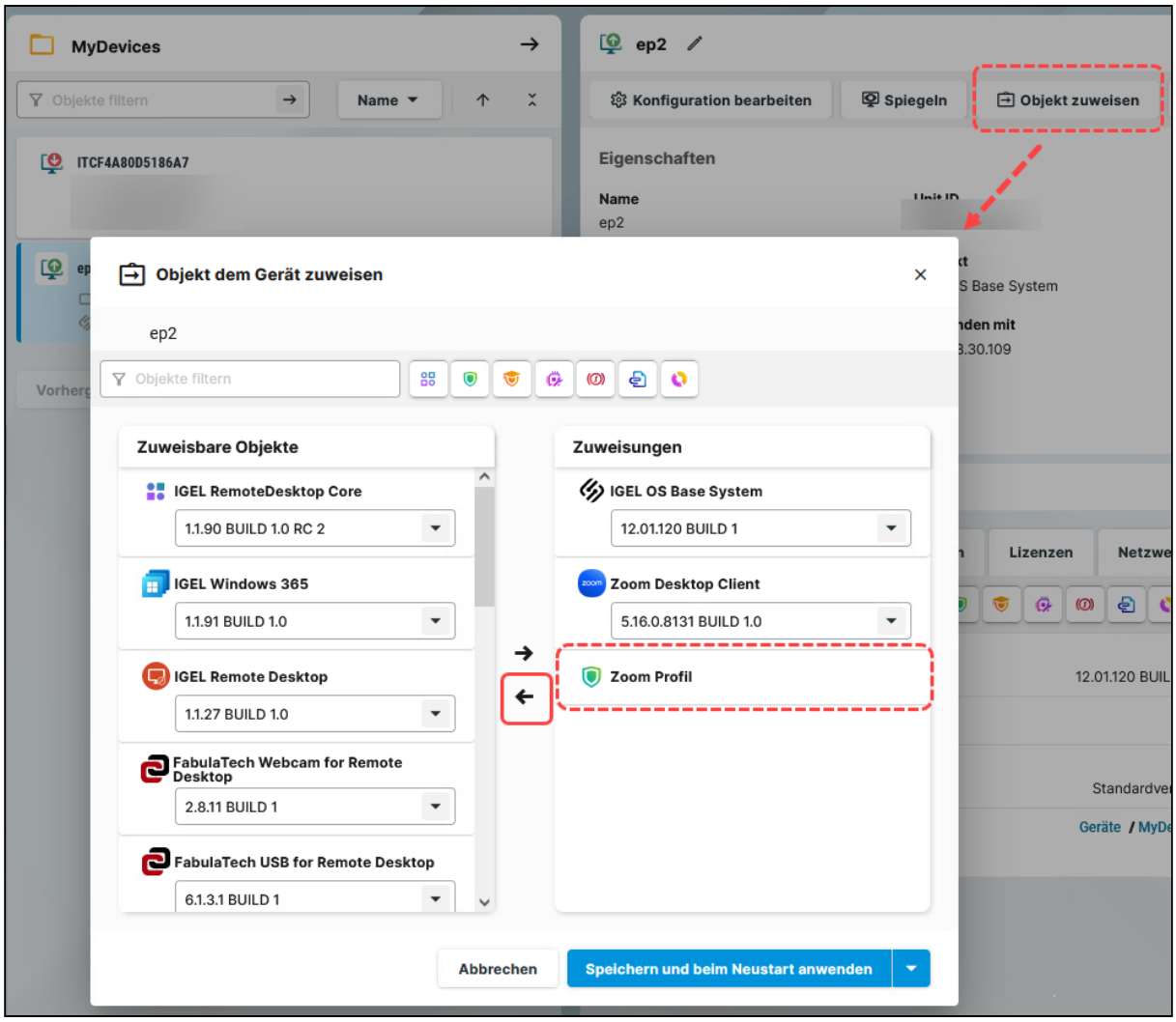
Um eine App von Ihrem Gerät zu entfernen, gehen Sie wie folgt vor:

1. Wählen Sie unter **Geräte** das Gerät / Geräteverzeichnis aus, von dem Sie eine App entfernen möchten, und klicken Sie **Objekt zuweisen**.

2. Wählen Sie die zu entfernende App oder im Falle der impliziten App-Zuweisung ein Profil aus, über das diese App auf dem Gerät installiert ist, und klicken Sie auf die linke Pfeiltaste.
   Im Falle der expliziten App-Zuweisung:



Im Falle der impliziten App-Zuweisung:



3. Entscheiden Sie, ob die neuen Einstellungen sofort oder erst beim nächsten Neustart des Geräts wirksam werden sollen, und speichern Sie entsprechend.
   Wenn Sie das Background App Update (see page 893) aktiviert haben, muss stattdessen der Befehl **Update** gesendet werden.

Schnelle Objektentfernung

Alternativ können Sie über **Geräte > [Name des Geräts / Geräteverzeichnisses] > Zugewiesene Objekte** einfach zum Objekt navigieren, das Sie entfernen möchten, und auf die Schaltfläche **Objekt entfernen** klicken. Weitere Informationen finden Sie unter Objekte in der IGEL UMS Web App zuweisen (see page 815).

Apps in der IGEL UMS Web App löschen

In der IGEL Universal Management Suite (UMS) Web App können Sie den App-Pool bereinigen und nicht mehr benötigte Apps und App-Versionen löschen.

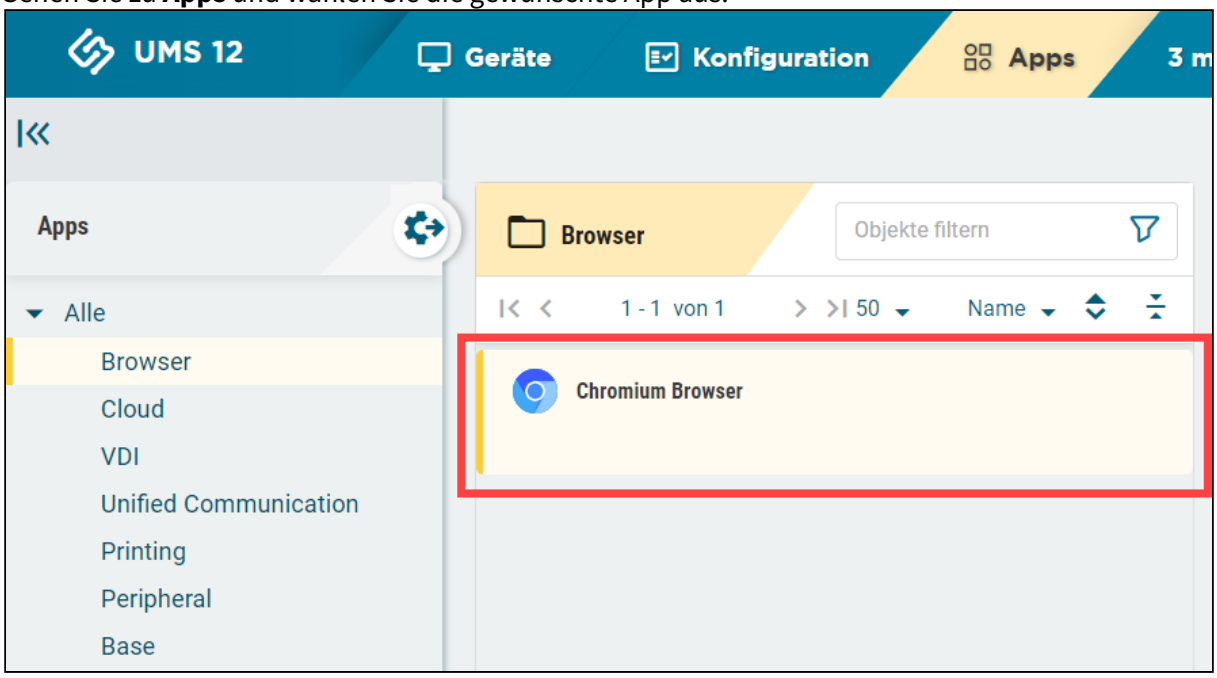
> Es können nur Apps / App-Versionen gelöscht werden, die nicht verwendet werden.
> Wenn Sie eine App / App-Version löschen, wird sie sofort aus der UMS entfernt, d.h. ohne Verschiebung in den Papierkorb.
> **Tipp**: Wenn alle Objekte, die eine App verwenden, gelöscht zu sein scheinen, aber die App trotzdem nicht entfernt werden kann, da das System sie als verwendet meldet, überprüfen Sie den Papierkorb auf Geräte und Profile, die die App noch verwenden können, und löschen Sie diese. Weitere Informationen zum Papierkorb finden Sie unter Papierkorb - Löschen von Objekten in der IGEL UMS (see page 545).

Menüpfad: **UMS Web App > Apps**

App-Version löschen

So löschen Sie eine App-Version:

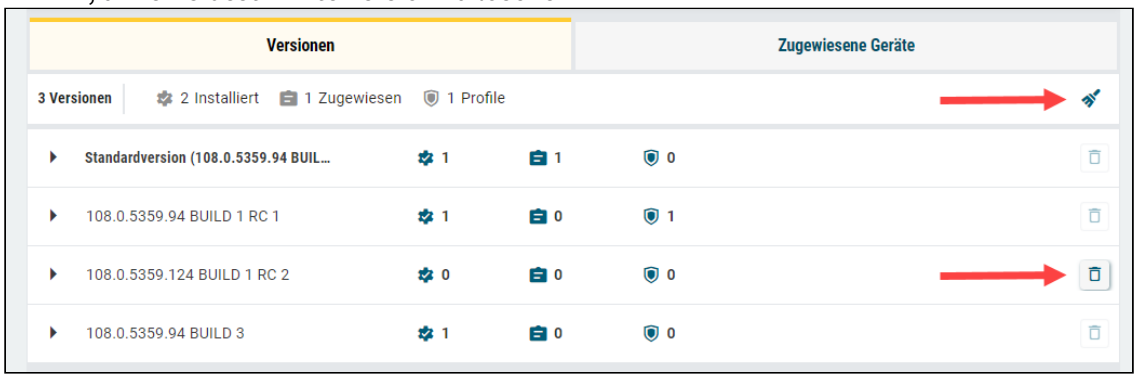
1. Gehen Sie zu **Apps** und wählen Sie die gewünschte App aus.



2. Klicken Sie **Versionen**.
   Alle verfügbaren Versionen werden angezeigt.

3. Klicken Sie

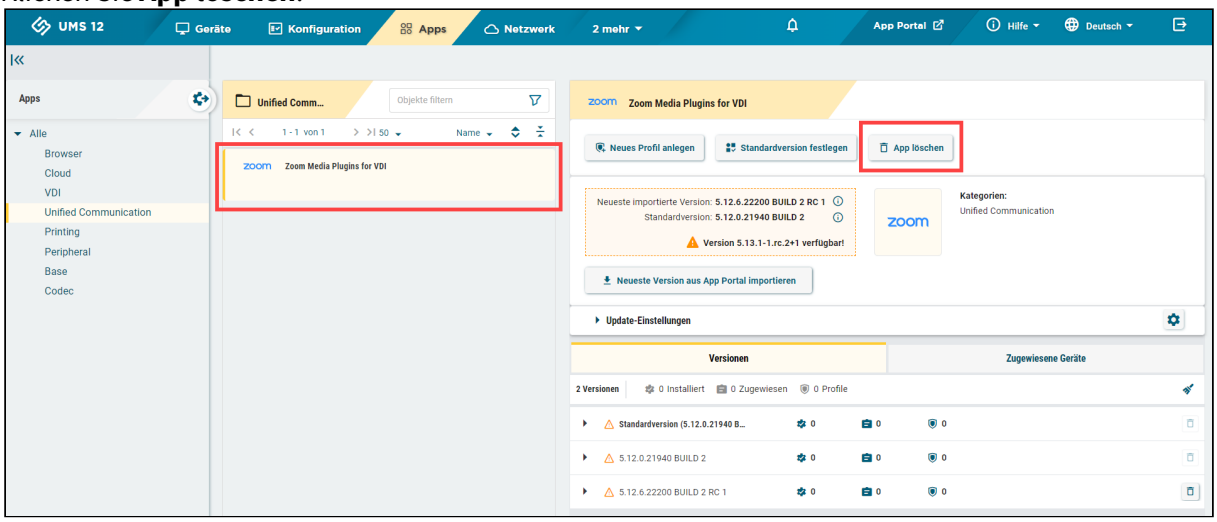
- das Bürstensymbol, um alle nicht verwendeten Versionen zu löschen, d.h. die nicht installiert, zugewiesen sind oder nicht in Profilen benutzt und als Standardversion festgelegt werden
-  , um eine bestimmte Version zu löschen



App löschen

So löschen Sie eine App:

1. Wählen Sie unter **Apps** die gewünschte App aus.
2. Klicken Sie **App löschen**.



Updating IGEL OS Apps

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

Configuring Global Settings for the Update of IGEL OS Apps

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

Configuring Update Settings for Individual IGEL OS Apps

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

How to Trigger the App Update in the IGEL UMS

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

Multistage Update of IGEL OS Base System

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

How to Configure the Background App Update in the IGEL UMS Web App

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

Export und Hochladen von Apps in der IGEL UMS

In der IGEL Universal Management Suite (UMS) Web App können Sie Apps exportieren und hochladen. Dies kann für Supportzwecke oder bei der Übertragung von App-Daten von einer UMS-Installation in eine andere hilfreich sein.

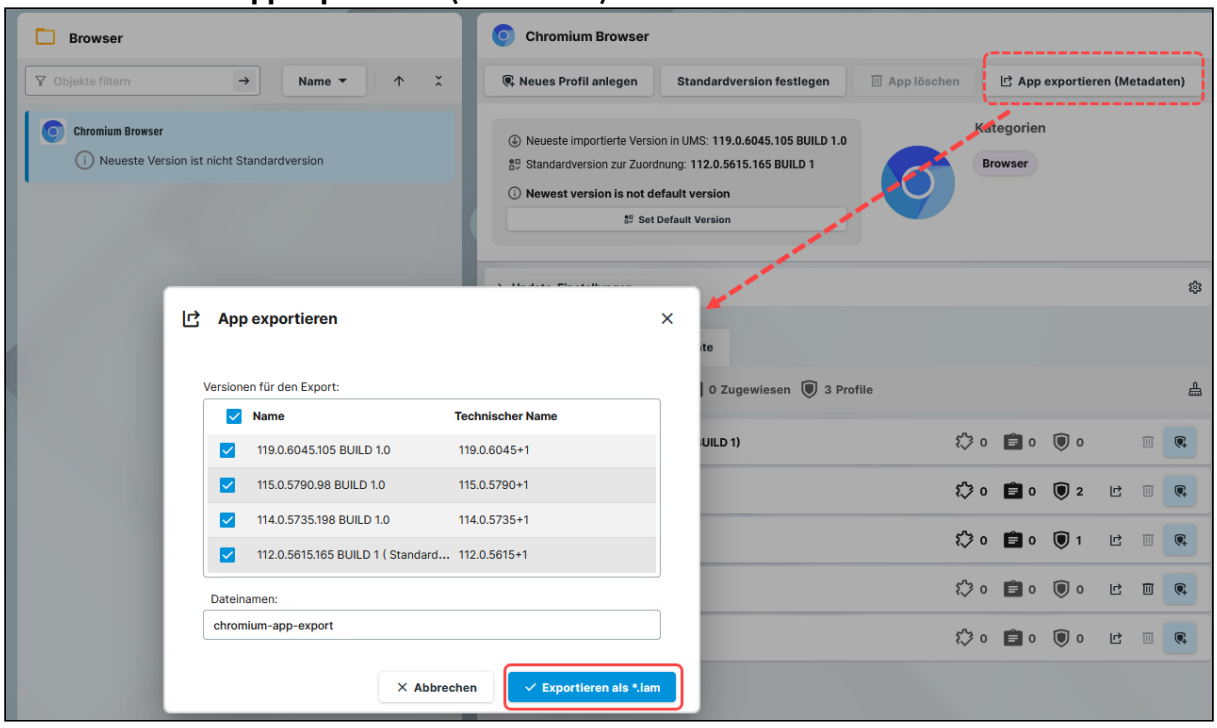
> Derzeit können nur Metadaten von Apps exportiert werden, d. h. keine Binärdateien.

Menüpfad: **UMS Web App > Apps**

Apps exportieren

So exportieren Sie eine App:

1. Wählen Sie unter **UMS Web App > Apps** die gewünschte App aus.
2. Klicken Sie **App exportieren (Metadaten)**.

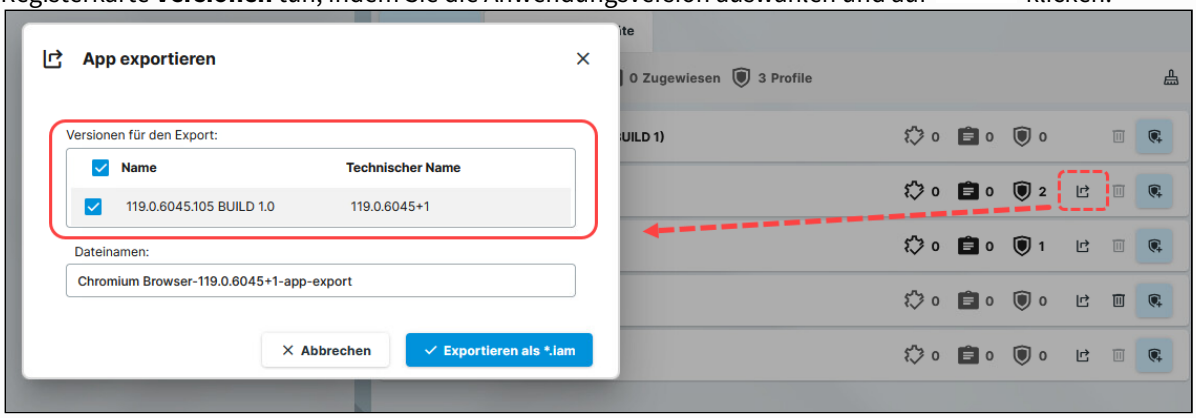


3. Wählen Sie die App-Versionen aus, die Sie exportieren möchten.

4. Geben Sie den **Dateinamen** an.

5. Bestätigen Sie den Export.
   Die Metadaten der markierten App-Version(en) werden in einer `.iam`-Datei gespeichert und können nun z. B. in eine andere UMS-Installation hochgeladen werden.

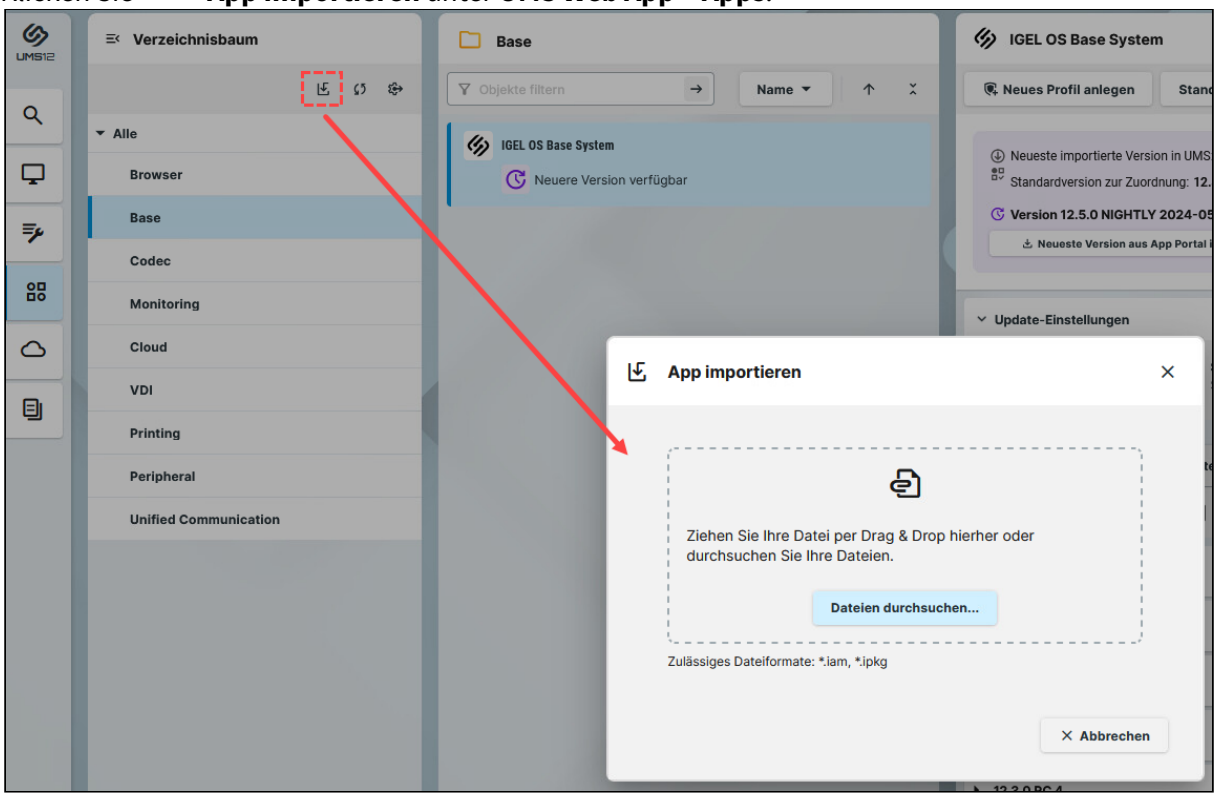
Wenn Sie eine bestimmte Version einer App exportieren möchten, können Sie dies auch auf der Registerkarte **Versionen** tun, indem Sie die Anwendungsversion auswählen und auf klicken.



Apps hochladen

So laden Sie eine App in die UMS hoch:

1. Klicken Sie  **App importieren** unter **UMS Web App > Apps**.



2. Wählen Sie die gewünschte Datei aus.

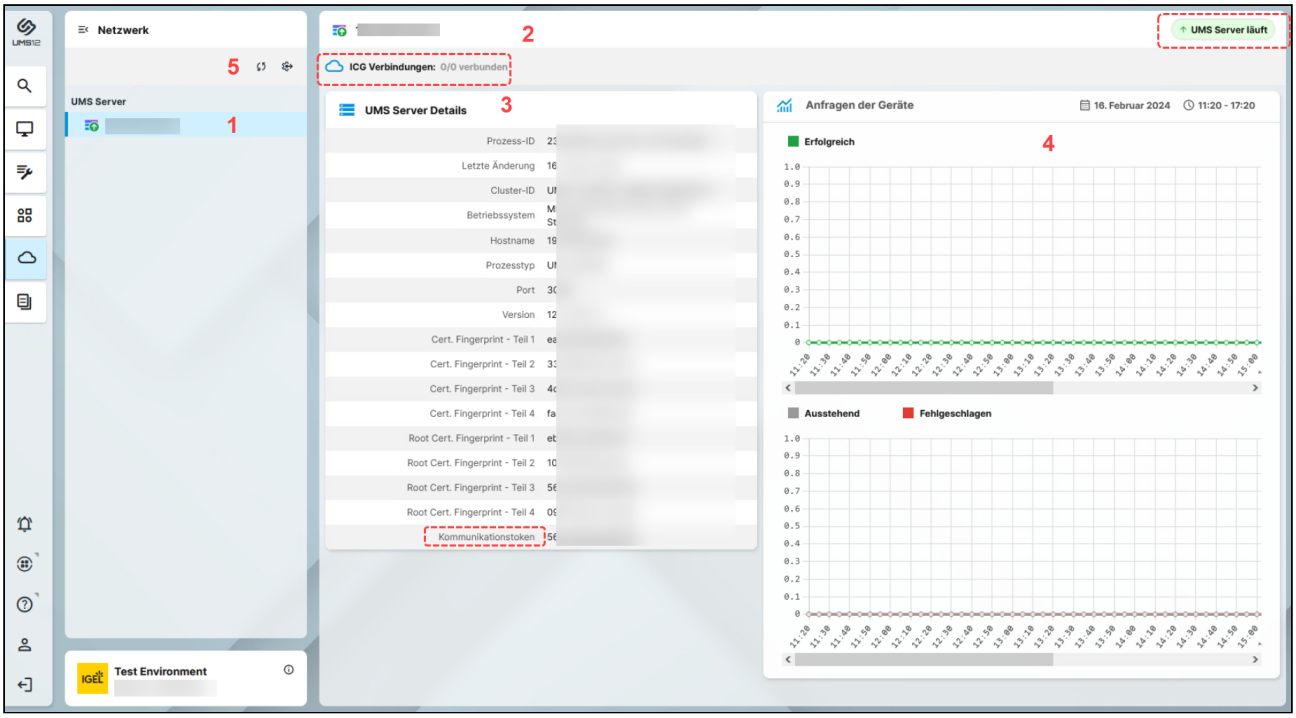
   Nur Dateien im `.iam` - und `.ipkg` -Format können hochgeladen werden.

3. Bestätigen Sie den Upload.
   Die hochgeladene App wird automatisch in dem entsprechenden App-Verzeichnis abgelegt. Sie können die App nun Ihren Endgeräten zuweisen oder Profile erstellen, die diese App konfigurieren.

Netzwerk-Einstellungen in der IGEL UMS Web App

Im Bereich **Netzwerk** der IGEL Universal Management Suite (UMS) Web App finden Sie Informationen zu allen angeschlossenen UMS Servern, UMS Load Balancern und IGEL Cloud Gateways. Hier können Sie auch die OBS-Routing-Details für den IGEL Onboarding Service finden und den Spitznamen für Ihre UMS festlegen.

Menüpfad: **UMS Web App > Netzwerk**



1	Liste aller verfügbaren UMS Server / UMS Load Balancer / IGEL Cloud Gateways (ICG)
2	In der Kopfzeile finden Sie die folgenden Angaben: • Status des ausgewählten UMS Servers / UMS Load Balancers / IGEL Cloud Gateways, siehe unten "Statusanzeigen". • Status der UMS Server- / ICG-Verbindungen (verbunden, nicht verbunden, unbekannt) • Anzahl der derzeit verbundenen Geräte (nur für das ICG)

3	Details zum ausgewählten UMS Server / UMS Load Balancer / IGEL Cloud Gateway ⓘ **Kommunikationstoken** finden Sie hier. Das Kommunikationstoken kann während des Onboarding-Prozesses verwendet werden. Weitere Informationen finden Sie unter Onboarding IGEL OS 12 Devices.
4	Statistik zu den Geräteanfragen
5	• Aktualisieren Sie die Netzwerkinformationen. • Öffnen Sie den Bereich **Einstellungen**. Siehe Details unten.

Statusanzeigen

UMS Server

Die folgenden Symbole zeigen den Status der installierten UMS Server an.

	Der UMS Server läuft.
	Der UMS Server läuft nicht.
	Der Status des UMS Servers ist unbekannt (z. B. wenn ein neuer Server im Netzwerk propagiert wird) oder wurde noch nicht geladen.
	Der Benutzer hat keine Berechtigungen, Details des UMS Servers zu sehen.
	Der UMS Server wird gerade aktualisiert.

UMS Load Balancer

Die folgenden Symbole zeigen den Status der installierten UMS Load Balancer an.

	Der Load Balancer läuft.
	Der Load Balancer läuft nicht.
	Der Status des UMS Load Balancers ist unbekannt (z. B. wenn ein neuer Load Balancer im Netzwerk propagiert wird) oder wurde noch nicht geladen.
	Der Benutzer hat keine Berechtigungen, Details des Load Balancers zu sehen.

	Der Load Balancer wird gerade aktualisiert.

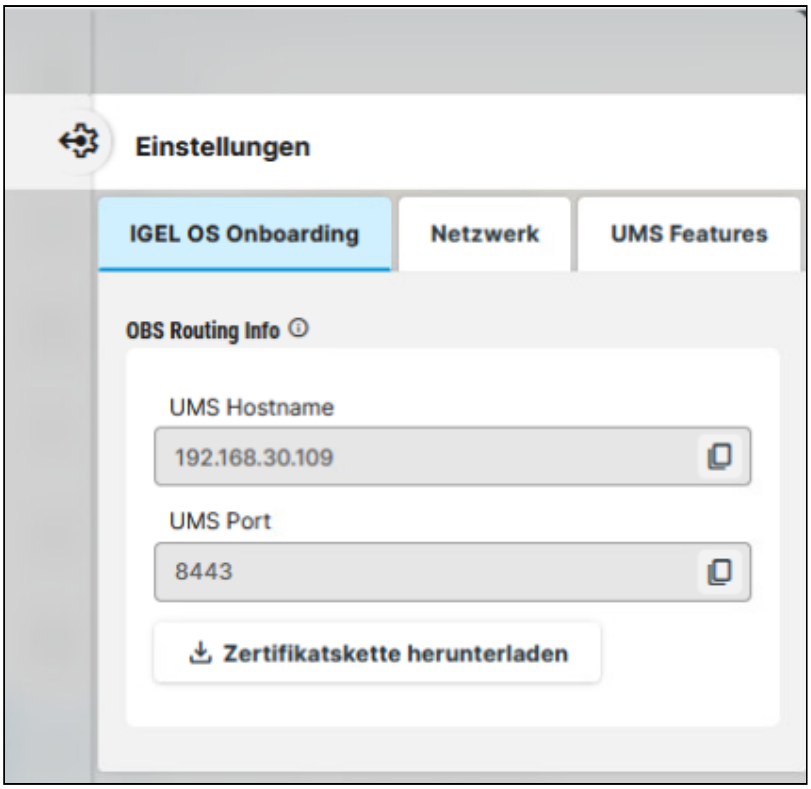
IGEL Cloud Gateway

Die folgenden Symbole zeigen den Status der installierten IGEL Cloud Gateways an.

	Das IGEL Cloud Gateway läuft.
	Das IGEL Cloud Gateway läuft nicht.
	Der Status des IGEL Cloud Gateways ist unbekannt oder wurde noch nicht geladen.
	Der Benutzer hat keine Berechtigungen, Details des IGEL Cloud Gateways zu sehen.
	Das IGEL Cloud Gateway wird gerade aktualisiert.

Einstellungen

Klicken Sie  , um den Bereich **Einstellungen** zu öffnen.



IGEL OS Onboarding

Hier finden Sie **OBS-Routing-Informationen**, die benötigt werden, wenn Sie den IGEL Onboarding Service (OBS) verwenden. Um die Daten zu kopieren, klicken Sie .

UMS Hostname

Hostname (Fully Qualified Domain Name) oder IP-Adresse des UMS Servers.

Falls konfiguriert, wird hier die Cluster-Adresse (see page 581) oder die Öffentliche Adresse (see page 551) verwendet (in der angegebenen Reihenfolge).

UMS Port

Port, unter dem die UMS erreicht werden kann. Der Standardport des UMS Webservers ist 8443, siehe Einstellungen - Servereinstellungen im IGEL UMS Administrator ändern (see page 709). Details zu den von der UMS verwendeten Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).

Falls konfiguriert, wird hier der Cluster-Address-Port (see page 581) oder der Öffentliche Web-Port (see page 551) verwendet (in der angegebenen Reihenfolge).

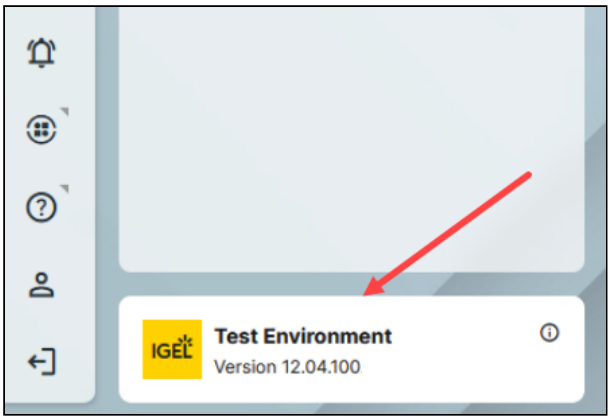
Zertifikatskette herunterladen

Lädt das UMS Stammzertifikat mit der `.crt`-Dateierweiterung herunter.

Netzwerk

Alias

Ein hier angegebener Name wird in der Menüleiste der UMS Web App sowie im Browser-Tab angezeigt und hilft, eine UMS-Instanz von einer anderen zu unterscheiden.



Um den Wert zu ändern, benötigen Sie die Berechtigung für den Knoten **Server-Netzwerkeinstellungen** unter **UMS Konsole > UMS Administration > Globale Konfiguration**.
Wie Sie Rechte festlegen können, erfahren Sie unter Zugriffsrechte im Administrationsbereich (see page 693).

UMS Features

Die Berechtigung für den Knoten **UMS Features** unter **UMS Konsole > UMS Administration > Globale Konfiguration** wird benötigt.
Wie Sie Rechte festlegen können, erfahren Sie unter Zugriffsrechte im Administrationsbereich (see page 693).

Templateprofile aktivieren

☑ Templateprofile werden aktiviert. Informationen zu Templateprofilen finden Sie unter Templateprofile in der IGEL UMS (see page 416).

Priority Profile aktivieren

☑ Priority Profile werden aktiviert. Informationen zu Priority Profilen finden Sie unter Priority Profile in der IGEL UMS (see page 413).

Aktiviere Insight Service

☑ Aktiviert den IGEL Insight Service, wenn Sie die Datenschutzrichtlinien in dem geöffneten Dialog akzeptieren und auf **Aktivieren** klicken. Wenn Sie den IGEL Insight Service aktivieren, sammelt IGEL spezifische Analyse- und Nutzungsdaten; siehe IGEL Insight Service.

☐ Deaktiviert den IGEL Insight Service.

Logging in der IGEL UMS Web App

Im Bereich **Logging** der IGEL Universal Management Suite (UMS) Web App können Sie die Protokollierung aktivieren und nach Protokollen gemäß den konfigurierten Suchparametern suchen.

> Nicht alle Aktionen, die in der UMS Konsole durchgeführt werden, werden in der UMS Web App angezeigt. Protokolle der UMS Web App werden in der UMS Konsole nicht angezeigt; wo sie zu finden sind, erfahren Sie unter Logging (see page 661).

> Löschen Sie regelmäßig nicht benötigte Protokolle, um Speicherplatzmangel vorzubeugen.

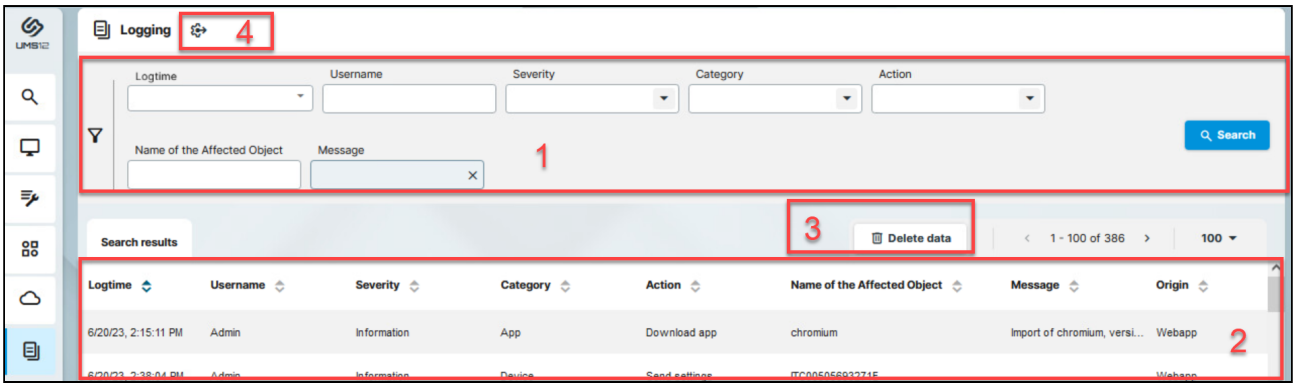
Menüpfad: **UMS Web App > Logging**

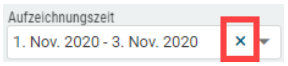
Protokolle sind verfügbar, wenn:

- Protokollierung ist aktiviert
  - unter **UMS Web App > Logging > Einstellungen**  (siehe unten)
    oder
  - unter **UMS Konsole > UMS Administration > Globale Konfiguration > Logging** (siehe Logging (see page 661))
- Ein Benutzer verfügt über ausreichende Rechte. Einzelheiten darüber, wo Sie Berechtigungen definieren können, finden Sie unter Allgemeine Administratorenrechte (see page 682) und Zugriffsrechte im Administrationsbereich (see page 693).

Die letzte Suchkonfiguration wird automatisch gespeichert und beim nächsten Aufruf des Bereiches **Logging** wiederhergestellt.

Wenn in der Suchmaske keine Werte angegeben werden, werden alle verfügbaren Protokollen angezeigt.

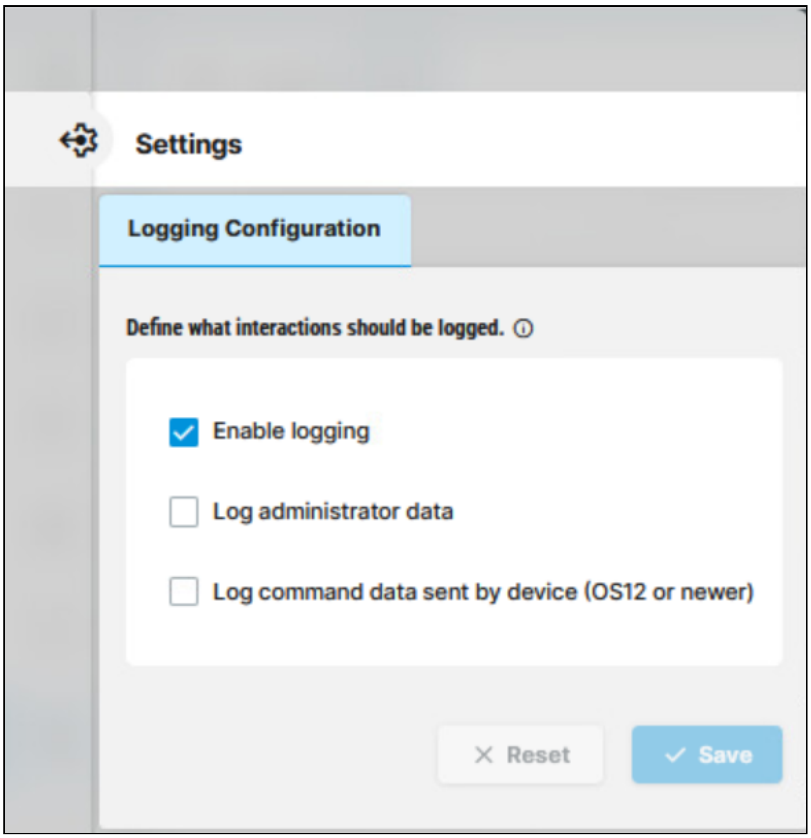


1	Suchmaske	Kriterien für die Suche der Protokolle (mit logischem *AND* verknüpft) Um einen Wert zu entfernen, klicken Sie auf  und dann auf **Suchen**. Dadurch werden die Suchergebnisse aktualisiert.
2	Suchtags	Zeigen die in der Suchmaske angegebenen Suchparameterwerte an. Wenn Sie in einen anderen Bereich, z. B. **Geräte**, und zurück wechseln, erkennen Sie an den Suchtags, dass die vorherige Suchkonfiguration noch aktiv ist.
3	Protokollliste	Zeigt alle Protokolle an, die den Suchkriterien entsprechen. • Paging für die Navigation in der Protokollliste • Anzahl der auf einer Seite anzuzeigenden Protokollnachrichten definieren • innerhalb jeder ausgewählten Spalte sortieren • Tooltipps, die im Falle von Abkürzungen hilfreich sind

4	Daten löschen	Löscht die Protokolle, die älter sind, als die angegebene Anzahl der Tage. ⚠ Um die Protokolle löschen zu können, muss ein Benutzer über die Berechtigung "Logging-Einträge löschen" verfügen, siehe Allgemeine Administratorenrechte (see page 682). Unmittelbar nach dem Löschen der Protokolle erscheint eine Meldung "`Es wurden keine passenden Logs gefunden`". Warten Sie auf das nächste Reindizieren, um die aktualisierte Liste der Protokollnachrichten anzusehen. Neue Protokolle, d.h. Protokolle für Aktionen, die nach dem Löschvorgang durchgeführt wurden, können Sie allerdings sofort ansehen und durchsuchen.
5	Einstellungen	Ermöglicht die Konfiguration der Protokollierungseinstellungen, siehe unten.

Einstellungen

▶ Klicken Sie  , um den Bereich **Einstellungen** zu öffnen.



Logging aktivieren

☑ Aktionen des UMS Benutzers werden protokolliert. Damit wird die Protokollierung für die UMS Konsole und für die UMS Web App aktiviert.

☐ Aktionen des UMS Benutzers werden nicht protokolliert. Damit wird die Protokollierung für die UMS Konsole und für die UMS Web App deaktiviert. (Standard)

Die folgenden Optionen sind verfügbar, wenn **Logging aktivieren** aktiviert ist:

Logging mit Benutzernamen

☑ Der Name des Administrators, der die Aktion gestartet hat, wird protokolliert. Damit wird die Protokollierung des Administratorennamens für die UMS Konsole aktiviert.

☐ Der Name des Administrators, der die Aktion gestartet hat, wird nicht protokolliert. Damit wird die Protokollierung des Administratorennamens für die UMS Konsole deaktiviert. (Standard)

Kommandos des Gerätes mitloggen (OS 12+)

☑ Von einem Gerät gestartete Aktionen (d.h. jeder Befehl, den ein IGEL OS 12-Gerät an die UMS sendet) werden protokolliert.

☐ Von einem Gerät gestartete Aktionen werden nicht protokolliert. (Standard)

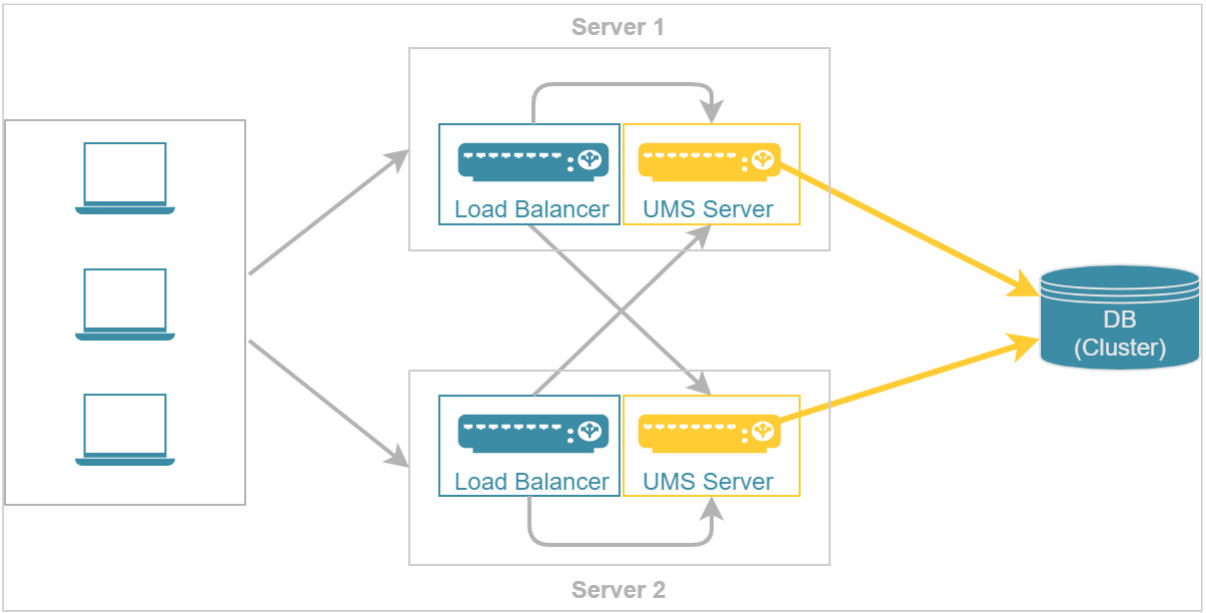
UMS Erweiterungen

High Availability (HA)

Die High-Availability-Erweiterung ist ein Bestandteil der IGEL UMS. Sie ist für große Umgebungen gedacht, in denen neue Einstellungen simultan ausgerollt werden müssen, oder in denen der ausfallsichere Rollout neuer Einstellungen geschäftskritisch ist. Die technische Umsetzung basiert auf einem Verbund mehrerer UMS Server.

Ein vorgeschalteter UMS Load Balancer übernimmt die Lastverteilung und stellt somit sicher, dass jedes Gerät jederzeit neue Einstellungen erhalten kann, auch wenn sich zum Arbeitsbeginn eine Vielzahl von Geräten gleichzeitig am UMS Server anmeldet und nach neuen Konfigurationsprofilen oder Firmwareupdates sucht. Hinsichtlich maximaler Prozesssicherheit und Hochverfügbarkeit empfiehlt IGEL, auch den UMS Load Balancer sowie die Datenbank redundant auszulegen.

Beispiel:



Siehe auch Konfigurationsoptionen (see page 911).

Lizenzierung mit dem Lizenzierungsmodell für IGEL OS 11

Die High-Availability-Erweiterung ist in der Workspace Edition enthalten, so dass Geräte mit IGEL OS 11 ein UMS High-Availability-Netzwerk ohne zusätzliche Lizenz nutzen können.

- Konfigurationsoptionen (see page 911)
- HA-Installation (see page 914)
- Installation eines HA-Netzwerks aktualisieren (see page 931)
- Lizenzierung der High-Availability-Erweiterung (see page 943)
- UMS HA Statusprüfung - Ihre High Availability- und Distributed UMS-Systeme analysieren (see page 944)
- IGEL UMS HA-Dienste und -Prozesse (see page 949)

Siehe auch die Artikelsammlung High Availability (see page 149).

Konfigurationsoptionen

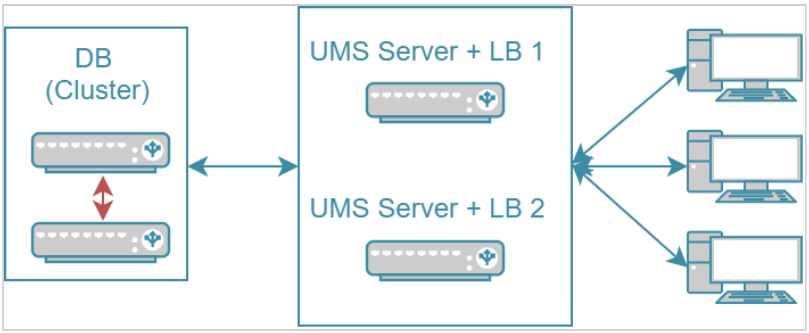
Bei der Planung der Konfiguration Ihres HA-Netzwerks (High Availability) müssen Sie entscheiden, ob Sie den UMS Server und den UMS Load Balancer auf demselben Host oder auf getrennten Hosts installieren möchten. Gleichzeitig stellt sich die Frage, wie viele UMS Server und UMS Load Balancer benötigt werden. Der folgende Artikel beschreibt die häufigsten Anwendungsfälle und bietet nur allgemeine Größenempfehlungen. Ihre individuelle Konfiguration kann davon abweichen.

> Bei der Entscheidung, wie viele UMS Server und Load Balancer Sie benötigen, reicht es nicht aus, nur Ihre Endgeräte zu zählen. Am wichtigsten ist, dass Sie die gesamte Netzwerkumgebung sowie die weiteren Gegebenheiten an Ihrem Arbeitsplatz analysieren. Siehe Leitlinien zur Installation und Größenbestimmung der IGEL UMS (see page 279) sowie IGEL UMS Größenangaben & Architekturdiagramme (see page 281) und wenden Sie sich für eine Beratung an Ihren IGEL Vertriebspartner.

UMS Server & UMS Load Balancer sind auf demselben Hostrechner installiert

Das typischste Szenario beim Einsatz der UMS High Availability ist die Installation des UMS Servers und des UMS Load Balancers auf demselben Hostrechner. UMS Server und UMS Load Balancer bieten Redundanz und sind auf zwei Servern installiert. Die Datenbank ist im Idealfall als Cluster ausgelegt.

Typische Anwendungsfälle	**#UMS Server + UMS Load Balancer**
Die Installation auf demselben Hostrechner ist in diesen Fällen geeignet: • Anzahl der Geräte < 50 000 • Sie verwenden das Feature Shared Workplace (see page 951)	2 UMS Server 2 UMS Load Balancer

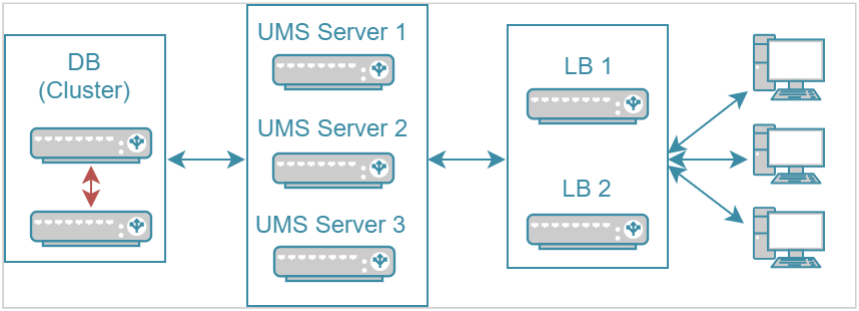


In dieser Konfiguration kann jeder der beiden Server auch allein die Aufgaben als UMS Server erfüllen. Sind beide Server gleichzeitig aktiv, ergibt sich eine Lastverteilung. Beachten Sie jedoch, dass neben dem eigentlichen UMS Server der Load Balancer zusätzlich Last erzeugt.

UMS Server & UMS Load Balancer sind auf getrennten Hostrechnern installiert

Wenn Sie eine sehr große Anzahl von Geräten verwalten müssen und/oder nicht möchten, dass die Serverressourcen zwischen dem Load Balancer und dem UMS Server geteilt werden, sollte die Installation auf getrennten Hosts in Betracht gezogen werden.

Typische Anwendungsfälle	**#UMS Server separat & Load Balancer separat**
Die Installation des Load Balancers auf einem separaten Hostrechner ist • erforderlich, wenn die Anzahl der Geräte > 50 000 • empfohlen, wenn Sie nicht möchten, dass der Load Balancer Ressourcen auf dem UMS Server-Host verbraucht	Die kleinste typische Konfiguration: 2-3 UMS Server 2 UMS Load Balancer Allgemeine Größenempfehlungen: • bis zu 6 UMS Server • bis zu 3 UMS Load Balancer • 1 UMS Server pro max. 50 000 Geräte • 1 LB pro max. 3 UMS Server



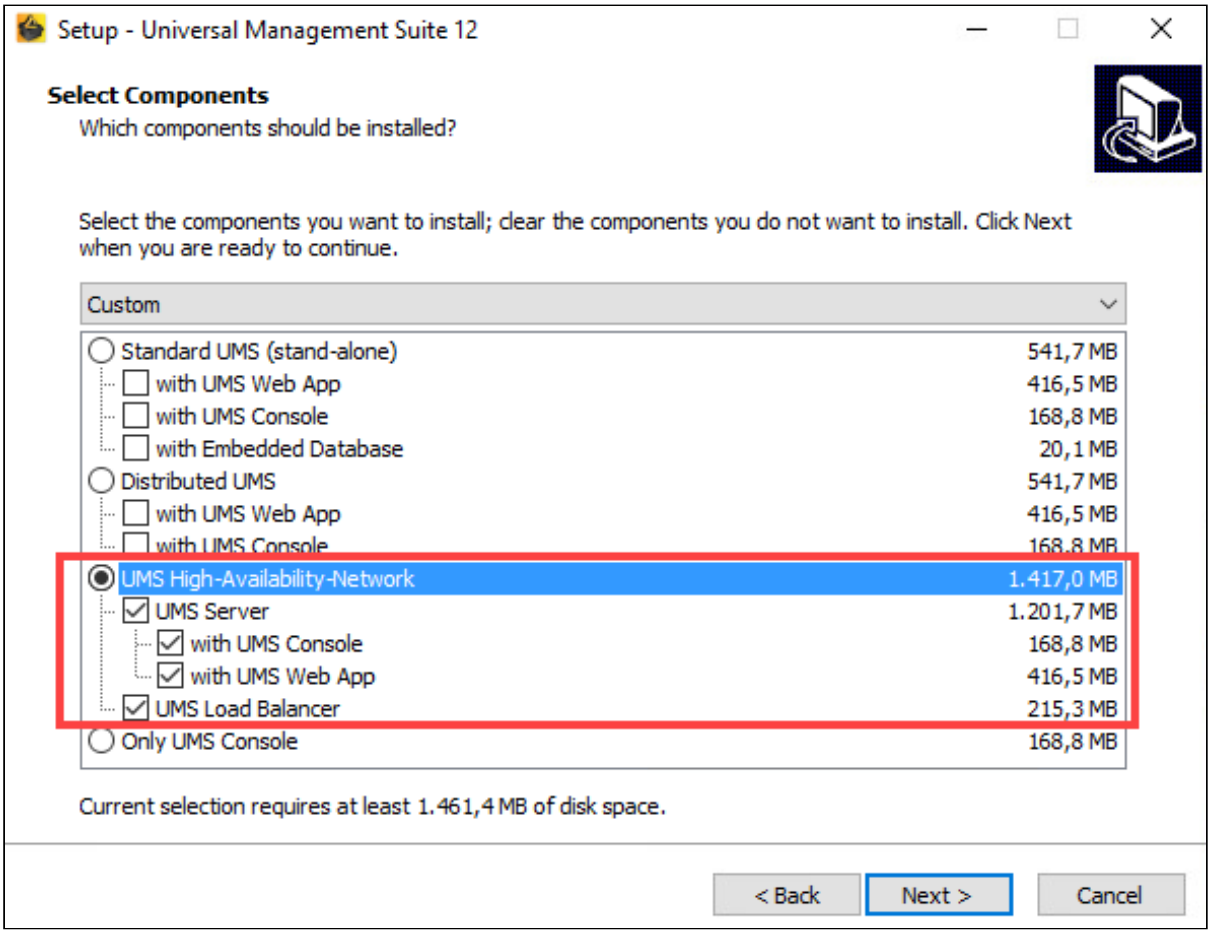
In der kleinsten typischen Konfiguration werden Anfragen von den Geräten von beiden Load Balancern an die UMS Server weitergereicht. Sollte einer der Load Balancer ausfallen, ist der andere weiterhin erreichbar und übernimmt die Kommunikation allein. Eine große Anzahl von Servern könnte einen einzigen Load Balancer überlasten und dieser würde selbst den Flaschenhals bilden. Daher sind nicht mehr als drei UMS Server in dieser Konfiguration vorgesehen. Für sehr große Installationen mit mehr als drei UMS Servern sollte die Zahl der Load Balancer entsprechend erhöht werden.

- High Availability mit IGEL UMS Load Balancern: Alle UMS Server und UMS Load Balancer müssen sich im **selben VLAN** befinden.
- Für High Availability (UMS HA) mit IGEL UMS Load Balancern muss der Netzwerkverkehr über den UDP-Broadcast-Port 6155 und der TCP-Verkehr sowie UDP-Broadcast-Verkehr über Port 61616 zugelassen werden. Weitere Informationen zu den UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).
- In der Netzwerkkonfiguration auf Windows-Servern muss die Option TCP/IPv6 für UMS 12 aktiviert sein.
- IGEL UMS HA Installation mit IGEL UMS Load Balancern wird in Cloud-Umgebungen wie Azure / AWS nicht unterstützt, da sie keinen Broadcast-Verkehr innerhalb ihrer Netzwerke

zulassen. Die HA-Installation ohne IGEL UMS Load Balancer (sowie die Distributed UMS (see page 246)) wird jedoch in Cloud-Umgebungen ab UMS Version 6.10 unterstützt.

HA-Installation

Für die Nutzung der High-Availability-Erweiterung müssen Sie die Option für die Installation der HA-Netzwerkkomponenten im UMS Installer auswählen.



Bei der Installation der High-Availability-Erweiterung ist es wichtig, zwischen der Installation des ersten HA-Servers und weiteren HA-Servern zu unterscheiden.

Bei der Installation des ersten HA-Servers (UMS Server obligatorisch) wird ein IGEL Netzwerktoken erstellt. Dieses Netzwerktoken ermöglicht die Integration neuer Server in dasselbe HA-Netzwerk und muss daher bei der Installation aller nachfolgenden HA-Server verwendet werden.

Folgen Sie diesen Anweisungen, um die High-Availability-Erweiterung zu installieren:

- HA: Installationsvoraussetzungen (see page 915)
- Ersten Server in einem HA-Netzwerk installieren (see page 917)
- Einem HA-Netzwerk weitere Server hinzufügen (see page 924)

Wie Sie die HA-Installation aktualisieren können, erfahren Sie unter Installation eines HA-Netzwerks aktualisieren (see page 931).

HA: Installationsvoraussetzungen

Um ein IGEL UMS High-Availability-Netzwerk installieren zu können, müssen folgende Mindestanforderungen an Hardware und Software erfüllt sein.

Die Installationsanforderungen können je nach der Größe Ihrer HA-Umgebung variieren. Weitere Informationen finden Sie unter Leitlinien zur Installation und Größenbestimmung der IGEL UMS (see page 279).

UMS High-Availability-Netzwerk: Mindestanforderungen

UMS Server (beinhaltet UMS Server, UMS Administrator und UMS Konsole)	**UMS Load Balancer**	**UMS Web App**	**Dateisystem**
UMS Server: • Mind. 4 GB RAM • Mind 2 GB freien HDD-Speicher UMS Konsole: • Mind. 3 GB RAM • Mind. 1 GB freien HDD-Speicher UMS Administrator: • Mind. 1 GB RAM	• Mind. 1 GB RAM • Mind. 1 GB freien HDD-Speicher	• 1 GB RAM • 1 GB freien HDD-Speicher	• 1 GB für die Programmdateien • Ca. 10 GB für jedes herunterzuladende Firmwareupdate
Informationen zu den unterstützten Betriebssystemen finden Sie im Abschnitt Supported Environment (see page 1047) der Release Notes.			

- Der UMS Server darf nicht auf einem Domänencontrollersystem installiert werden.
- Die manuelle Änderung von Java Runtime Environment auf dem UMS Server wird nicht empfohlen.
- Der Betrieb zusätzlicher Apache Tomcat Webserver zusammen mit dem UMS Server wird ebenfalls nicht empfohlen.

- High Availability mit IGEL UMS Load Balancern: Alle UMS Server und UMS Load Balancer müssen sich im **selben VLAN** befinden.
- Für High Availability (UMS HA) mit IGEL UMS Load Balancern muss der Netzwerkverkehr über den UDP-Broadcast-Port 6155 und der TCP-Verkehr sowie UDP-Broadcast-Verkehr

über Port 61616 zugelassen werden. Weitere Informationen zu den UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).
- In der Netzwerkkonfiguration auf Windows-Servern muss die Option TCP/IPv6 für UMS 12 aktiviert sein.
- IGEL UMS HA Installation mit IGEL UMS Load Balancern wird in Cloud-Umgebungen wie Azure / AWS nicht unterstützt, da sie keinen Broadcast-Verkehr innerhalb ihrer Netzwerke zulassen. Die HA-Installation ohne IGEL UMS Load Balancer (sowie die Distributed UMS (see page 246)) wird jedoch in Cloud-Umgebungen ab UMS Version 6.10 unterstützt.

Falls Sie einen externen Load Balancer / Reverse Proxy verwenden
Der FQDN und Port Ihres externen Load Balancers / Reverse Proxy muss in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Server-Netzwerkeinstellungen > Cluster-Adresse** angegeben werden. Informationen zur Cluster-Adresse finden Sie unter Server-Netzwerkeinstellungen in der IGEL UMS (see page 581).

Datenbanksysteme (DBMS)

Angaben zu den unterstützten Datenbanksystemen finden Sie in den Release Notes (see page 965) im Bereich "Supported Environment". Die Installations- und Betriebsvoraussetzungen für die Datenbank finden Sie in der Dokumentation des jeweiligen DBMS.

Die Embedded-Datenbank kann **nicht** für ein HA-Netzwerk verwendet werden. Sie können die Embedded-Datenbank für eine reine Testinstallation mit nur einem einzigen Server für UMS Server und Load Balancer verwenden.

Das Datenbanksystem muss für alle UMS Server zugänglich sein.

Ersten Server in einem HA-Netzwerk installieren

Voraussetzungen

- Eine Reihe von Servern mit dem von der UMS unterstützten Betriebssystem; siehe den Bereich "Supported Environment" in den Release Notes (see page 965).
- Ein von der UMS unterstütztes Datenbanksystem; siehe den Bereich "Supported Environment" in den Release Notes (see page 965).
- Alle Installationsanforderungen, die unter HA: Installationsvoraussetzungen (see page 915) beschriebenen sind, sind erfüllt.
- Die aktuelle Version der UMS ist vom IGEL Downloadserver[39] heruntergeladen.

Für die Erstinstallation ist es ratsam, einen Server ohne bestehende UMS Installation zu verwenden.

Anleitung

Um die UMS High-Availability-Erweiterung (HA) auf dem ersten Server zu installieren, folgen Sie den Anweisungen in der angegebenen Reihenfolge:

1. Eine Datenbank vorbereiten (see page 917)
2. Server vorbereiten (see page 917)
3. Die Installation starten (see page 918)
4. Die Datenbank anbinden (see page 921)
5. Die Installation überprüfen (see page 922)
6. Das IGEL Netzwerktoken speichern (see page 923)

Eine Datenbank vorbereiten

▶ Erstellen Sie ein Datenbankschema und einen Benutzer für die UMS. Verwenden Sie das entsprechende DBMS-Programm und dessen Dokumentation. Siehe auch Anbindung externer Datenbanksysteme (see page 308).

Server vorbereiten

1. Stellen Sie sicher, dass jeder Server die anderen über das Netzwerk "sehen" kann.

   - High Availability mit IGEL UMS Load Balancern: Alle UMS Server und UMS Load Balancer müssen sich im **selben VLAN** befinden.
   - Für High Availability (UMS HA) mit IGEL UMS Load Balancern muss der Netzwerkverkehr über den UDP-Broadcast-Port 6155 und der TCP-Verkehr sowie UDP-Broadcast-Verkehr über Port 61616 zugelassen werden. Weitere Informationen zu den UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).
   - In der Netzwerkkonfiguration auf Windows-Servern muss die Option TCP/IPv6 für UMS 12 aktiviert sein.

39 https://www.igel.com/software-downloads/

- IGEL UMS HA Installation mit IGEL UMS Load Balancern wird in Cloud-Umgebungen wie Azure / AWS nicht unterstützt, da sie keinen Broadcast-Verkehr innerhalb ihrer Netzwerke zulassen. Die HA-Installation ohne IGEL UMS Load Balancer (sowie die Distributed UMS (see page 246)) wird jedoch in Cloud-Umgebungen ab UMS Version 6.10 unterstützt.

2. Überprüfen Sie, ob die Zeit auf allen Servern synchronisiert ist.

   ⚠ Um Probleme mit Ihrer HA-Installation zu vermeiden, stellen Sie sicher, dass der Zeitunterschied auf den Servern des HA-Netzwerks eine Minute nicht überschreitet. Nach jeder manuellen Zeitänderung müssen die HA-Dienste auf dem entsprechenden Server neu gestartet werden.

3. Auf Linux-Systemen machen Sie das Verzeichnis `/root` für den Benutzer `root` schreibbar.

Die Installation starten

1. Starten Sie den UMS Installer.

   ⓘ Sie benötigen Administrationsrechte, um IGEL UMS HA installieren zu können.

2. Lesen und bestätigen Sie die Lizenzvereinbarung unter **License Agreement**.
3. Lesen Sie die **Information** über den Installationsprozess.
4. Wählen Sie einen Pfad für die Installation.
5. Wählen Sie je nach Ihrer gewünschten HA-Netzwerkkonfiguration (see page 911) die zu installierenden Komponenten: **UMS Server + UMS Load Balancer** oder **UMS Server**.

   ⚠ **UMS Server und UMS Load Balancer auf separaten Servern installieren**

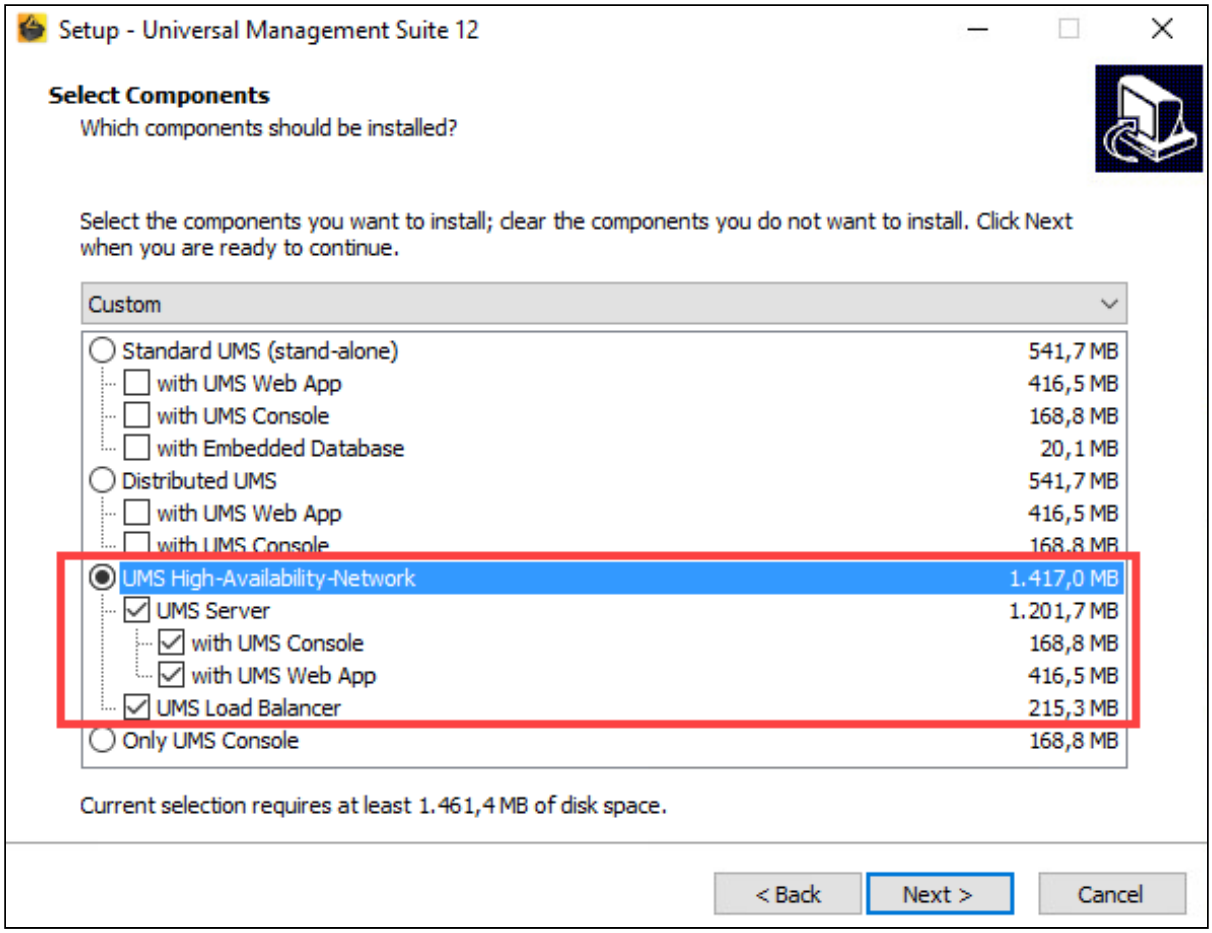
   Wenn Sie HA-Netzwerkkomponenten auf getrennten Servern installieren, muss **UMS Server** immer zuerst installiert werden. In diesem Fall wird das IGEL Netzwerktoken erstellt, das für die Integration weiterer Server in das HA-Netzwerk benötigt wird. Zusätzlich wird auch die Anwendung UMS Administrator installiert, die für die weitere Verwaltung der Installation erforderlich ist. Nach der Konfiguration und Aktivierung der Datenbank über den UMS Administrator wird der UMS Server im HA-Netzwerk verfügbar sein.
   Wird ein UMS Load Balancer einzeln installiert, werden weder das IGEL Netzwerktoken noch die UMS Konsole noch der UMS Administrator installiert. Lediglich die Option zur Deinstallation der UMS wird im Windows-Startmenü angelegt.

   ⓘ
   - Für die Verwaltung der UMS-Installation benötigen Sie die UMS Konsole. Bei Multiinstanz-Installationen muss die UMS Konsole nicht unbedingt auf jedem UMS Server installiert sein.

Hinweis: Aus Sicherheits-, Leistungs- oder anderen Gründen wird die UMS Konsole häufig zusätzlich auf einem separaten Host installiert.

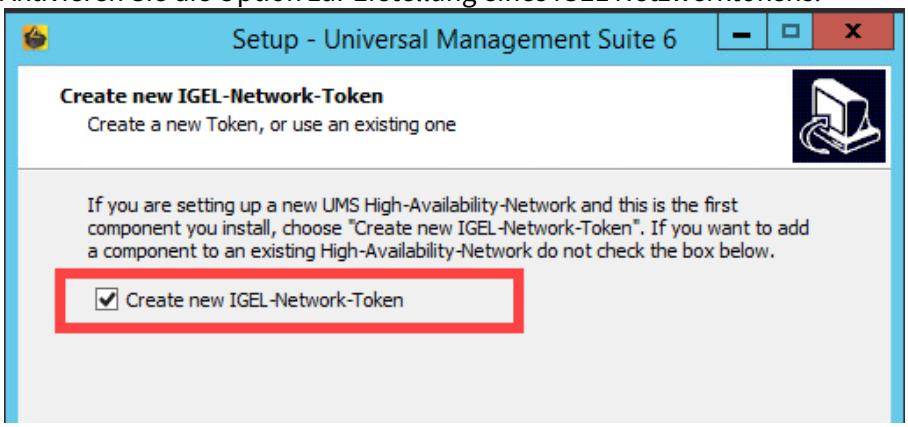
- Ohne die UMS Web App können Sie keine IGEL OS 12-Geräte verwalten. Daher muss die UMS Web App bei der Installation der UMS ausgewählt werden. Bei Multiinstanz-Installationen muss die UMS Web App nicht unbedingt auf jedem UMS Server installiert sein, siehe Wichtige Informationen zur IGEL UMS Web App (see page 784).
- Bei der Installation des UMS Servers wird automatisch die Anwendung UMS Administrator installiert, die für die Verwaltung der UMS-Installation erforderlich ist.

Informationen zu den Komponenten der UMS finden Sie unter Überblick über die IGEL UMS (see page 238).



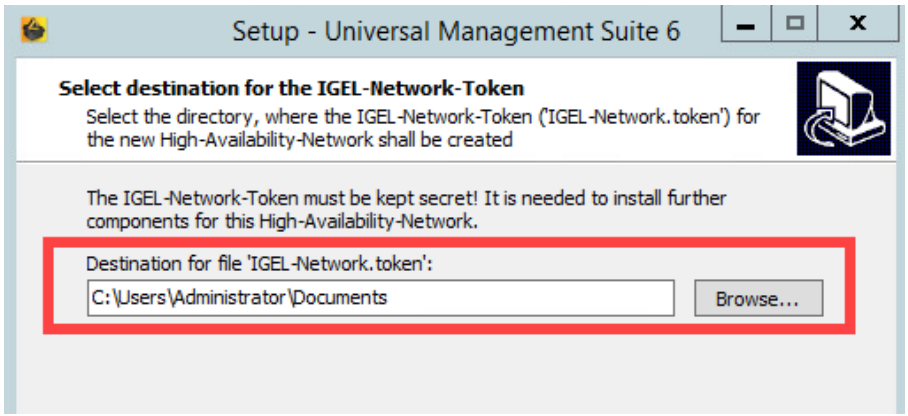
6. Bestätigen Sie den Dialog, dass Ihr System die angezeigten Systemanforderungen erfüllt.
7. Wählen Sie unter **UMS data directory** das Verzeichnis, in dem Universal Firmware Updates und Dateien gespeichert werden sollen.

8. Aktivieren Sie die Option zur Erstellung eines IGEL Netzwerktokens.



9. Geben Sie ein Verzeichnis zum Speichern des IGEL Netzwerktokens an. Das Verzeichnis muss für den Administrator schreibbar sein.

> ⚠ Bewahren Sie das IGEL Netzwerktoken an einem sicheren Ort auf! Es wird für alle nachfolgenden Serverinstallationen benötigt. Bei Verlust des IGEL Netzwerktokens muss die komplette Installation erneut gestartet werden.



10. Optional: Unter **Import existing keystore** können Sie die Datei `tc.keystore` aus einer bestehenden UMS Installation laden.

> ⚠ Diese Funktion kann Ihre UMS Installation zerstören. Importieren Sie diese Datei nur, wenn Sie genau wissen, was Sie tun.

11. Wenn die interne Windows Firewall auf dem Hostrechner aktiv ist: Überprüfen Sie die Einstellungen unter **Windows firewall settings** und ändern Sie diese, falls nötig. Jeder Port, der hier aktiviert ist, wird in der Windows Firewall auf dem Hostrechner des UMS Servers als Regel definiert.

> ⓘ **UMS 12 Kommunikationsports**

Wenn Sie Änderungen am Netzwerk vornehmen möchten, sollten Sie die folgenden Ports und Pfade berücksichtigen:

- Für IGEL OS 12-Geräte ist TCP 8443 /device-connector/* erforderlich.
  SSL kann am Reverse Proxy / externen Load Balancer (siehe IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading) oder am UMS Server terminiert werden.
- Für den Import von IGEL OS 12 Apps vom IGEL App Portal in die UMS ist die URL https://app.igel.com/ (TCP 443) erforderlich.
- Für die UMS Web App sind TCP 8443 /webapp/* und /wums-app/* erforderlich.
- Für die UMS Konsole ist der Root erforderlich, d. h. TCP 8443 /*
- Für IGEL OS 11-Geräte sind TCP 30001 und TCP/UDP 30005 erforderlich.

Weitere Informationen zu UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).

12. Geben Sie unter **Select Start Menu Folder** einen Ordnernamen für die Verknüpfung an.

13. Wählen Sie unter **Select Additional Tasks**, ob Sie auf dem Desktop Verknüpfungen für UMS Konsole und UMS Administrator (see page 707) anlegen möchten.

14. Lesen Sie die Zusammenfassung und starten Sie den Installationsprozess.

15. Schließen Sie den UMS Installer nach Abschluss der Installation.
    Der UMS Installer erstellt Einträge im Windows-Softwareverzeichnis und im Startmenü. Wenn dies ausgewählt wurde, werden auch Verknüpfungen für die UMS Konsole und den UMS Administrator auf dem Desktop abgelegt.

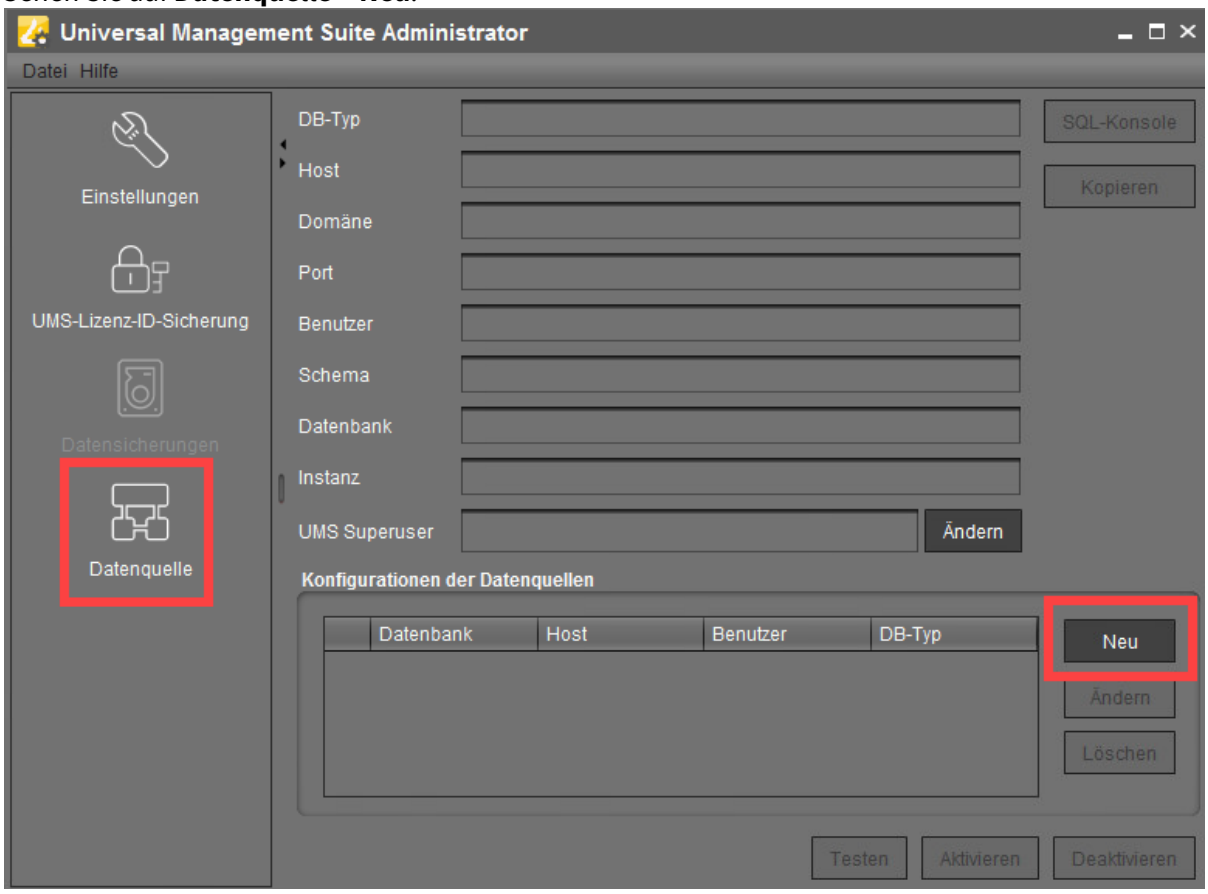
    Wird SQL Server AD nativ (see page 917) verwendet, müssen Sie auch den richtigen Starttyp und die richtigen Anmeldedaten für den Dienst "IGEL RMGUIServer" einstellen und den Dienst neu starten. Für Details siehe "Windows-Dienst für UMS Server konfigurieren" unter "UMS für SQL Server AD nativ einrichten" (see page 917).

Die Datenbank anbinden

1. Öffnen Sie den UMS Administrator.

   Standardpfad zum UMS Administrator:
   Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
   Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
   Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

2. Gehen Sie auf **Datenquelle > Neu**.



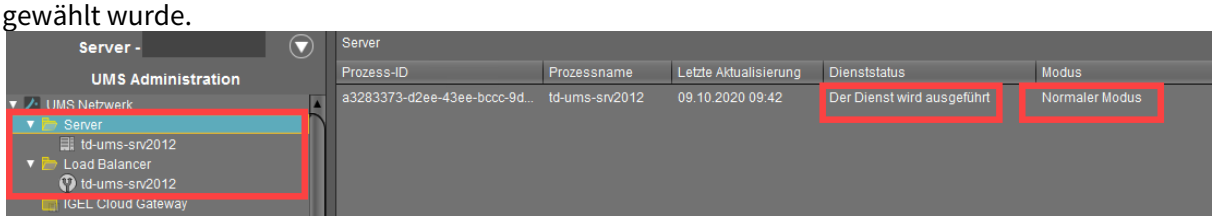
3. Geben Sie die Verbindungsangaben des vorbereiteten Datenbankschemas ein.
   Siehe auch Wie kann ich eine Datenquelle im IGEL UMS Administrator einrichten? (see page 730).

4. Klicken Sie **Aktivieren**, um die Datenquelle zu aktivieren. Siehe auch Datenquelle aktivieren (see page 734).

Die Installation überprüfen

1. Prüfen Sie, ob alle Prozesse laufen. Die Liste der Prozesse für UMS HA finden Sie unter IGEL UMS HA-Dienste und -Prozesse (see page 949).

2. Gehen Sie in der UMS Konsole auf **UMS Administration > UMS Netzwerk** und überprüfen Sie die Knoten **Server** und **Load Balancer**, wenn die komplette UMS HA-Erweiterung für die Installation gewählt wurde.



Das IGEL Netzwerktoken speichern

▶ Speichern Sie das IGEL Netzwerktoken, d.h. die Datei `IGEL-Network.token`, auf einem Speichermedium, das bei der Installation weiterer HA-Server zugänglich sein wird (z. B. im Netzwerk oder auf einem tragbaren Speichermedium wie einem USB-Stick). Bewahren Sie das IGEL Netzwerktoken stets gut geschützt auf.

Nächster Schritt

>> Fahren Sie mit dem Hinzufügen eines weiteren Servers zur HA-Installation fort, siehe Einem HA-Netzwerk weitere Server hinzufügen (see page 924).

Einem HA-Netzwerk weitere Server hinzufügen

Einführung

Weitere HA-Server – egal ob UMS Server, UMS Load Balancer oder beide gleichzeitig – werden analog zum ersten HA-Server installiert. Allerdings müssen Sie kein neues IGEL Netzwerktoken erstellen. Stattdessen wählen Sie das Netzwerktoken aus, das zuvor bei der Installation des ersten Servers in einem HA-Netzwerk angelegt wurde.

Zudem muss die Verbindung mit der selben Datenbank hergestellt werden, die vom ersten Server verwendet wird. Das UMS HA-Netzwerk funktioniert nur, wenn alle Server mit der gleichen Datenbank verbunden sind.

Voraussetzungen

- Eine HA-Installation (High-Availability) mit einer konfigurierten Datenbank, siehe Ersten Server in einem HA-Netzwerk installieren (see page 917).

  ⚠ Die Datenbankverbindung sollte bei der Installation des ersten UMS Servers in einem HA-Netzwerk definiert werden. In diesem Fall werden alle relevanten Konfigurationsinformationen automatisch auf die zusätzlichen UMS Server übertragen.

- Das IGEL Netzwerktoken, das während der Installation des ersten Servers in einem HA-Netzwerk erstellt wurde, siehe Ersten Server in einem HA-Netzwerk installieren (see page 918).
- Ein Server mit dem von der UMS unterstützten Betriebssystem; siehe den Bereich "Supported Environment" in den Release Notes (see page 965).
- Alle Installationsanforderungen, die unter HA: Installationsvoraussetzungen (see page 915) beschriebenen sind, sind erfüllt.
- Die gleiche Version der IGEL UMS wie für den ersten HA-Server ist vom IGEL Downloadserver[40] heruntergeladen.

Anleitung

Um der UMS HA-Installation einen neuen Server hinzuzufügen, folgen Sie den Anweisungen in der angegebenen Reihenfolge:

1. Den Server vorbereiten (see page 924)
2. Das IGEL Netzwerktoken vorbereiten (see page 925)
3. Die Installation starten (see page 925)
4. Die Installation überprüfen (see page 928)

Den Server vorbereiten

1. Stellen Sie sicher, dass der Server die anderen über das Netzwerk "sehen" kann.

   ⚠
   - High Availability mit IGEL UMS Load Balancern: Alle UMS Server und UMS Load Balancer müssen sich im **selben VLAN** befinden.

40 https://www.igel.com/software-downloads/

- Für High Availability (UMS HA) mit IGEL UMS Load Balancern muss der Netzwerkverkehr über den UDP-Broadcast-Port 6155 und der TCP-Verkehr sowie UDP-Broadcast-Verkehr über Port 61616 zugelassen werden. Weitere Informationen zu den UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).
- In der Netzwerkkonfiguration auf Windows-Servern muss die Option TCP/IPv6 für UMS 12 aktiviert sein.
- IGEL UMS HA Installation mit IGEL UMS Load Balancern wird in Cloud-Umgebungen wie Azure / AWS nicht unterstützt, da sie keinen Broadcast-Verkehr innerhalb ihrer Netzwerke zulassen. Die HA-Installation ohne IGEL UMS Load Balancer (sowie die Distributed UMS (see page 246)) wird jedoch in Cloud-Umgebungen ab UMS Version 6.10 unterstützt.

2. Überprüfen Sie, ob die Zeit auf allen Servern synchronisiert ist.

   ⚠ Um Probleme mit Ihrer HA-Installation zu vermeiden, stellen Sie sicher, dass der Zeitunterschied auf den Servern des HA-Netzwerks eine Minute nicht überschreitet. Nach jeder manuellen Zeitänderung müssen die HA-Dienste auf dem entsprechenden Server neu gestartet werden.

3. Auf Linux-Systemen machen Sie das Verzeichnis `/root` für den Benutzer `root` schreibbar.

Das IGEL Netzwerktoken vorbereiten

▶ Falls noch nicht geschehen, speichern Sie das IGEL Netzwerktoken, das während der Installation des ersten HA-Servers angelegt wurde, z.B. auf einem tragbaren Speichermedium.

ⓘ Wenn der Pfad nicht geändert wurde, befindet sich die Datei `IGEL-Network.token` standardmäßig im Home-Verzeichnis des Administratorbenutzers auf einem UMS Server-Host.

⚠ Wenn Sie bereits ein voll funktionsfähiges UMS HA-Netzwerk im Einsatz haben und dieses lediglich um einen weiteren HA-Server erweitern möchten, stellen Sie sicher, dass Sie für die zusätzliche HA-Server-Installation das **aktuelle** Netzwerktoken benutzen.
Wenn Sie es nicht gespeichert haben:

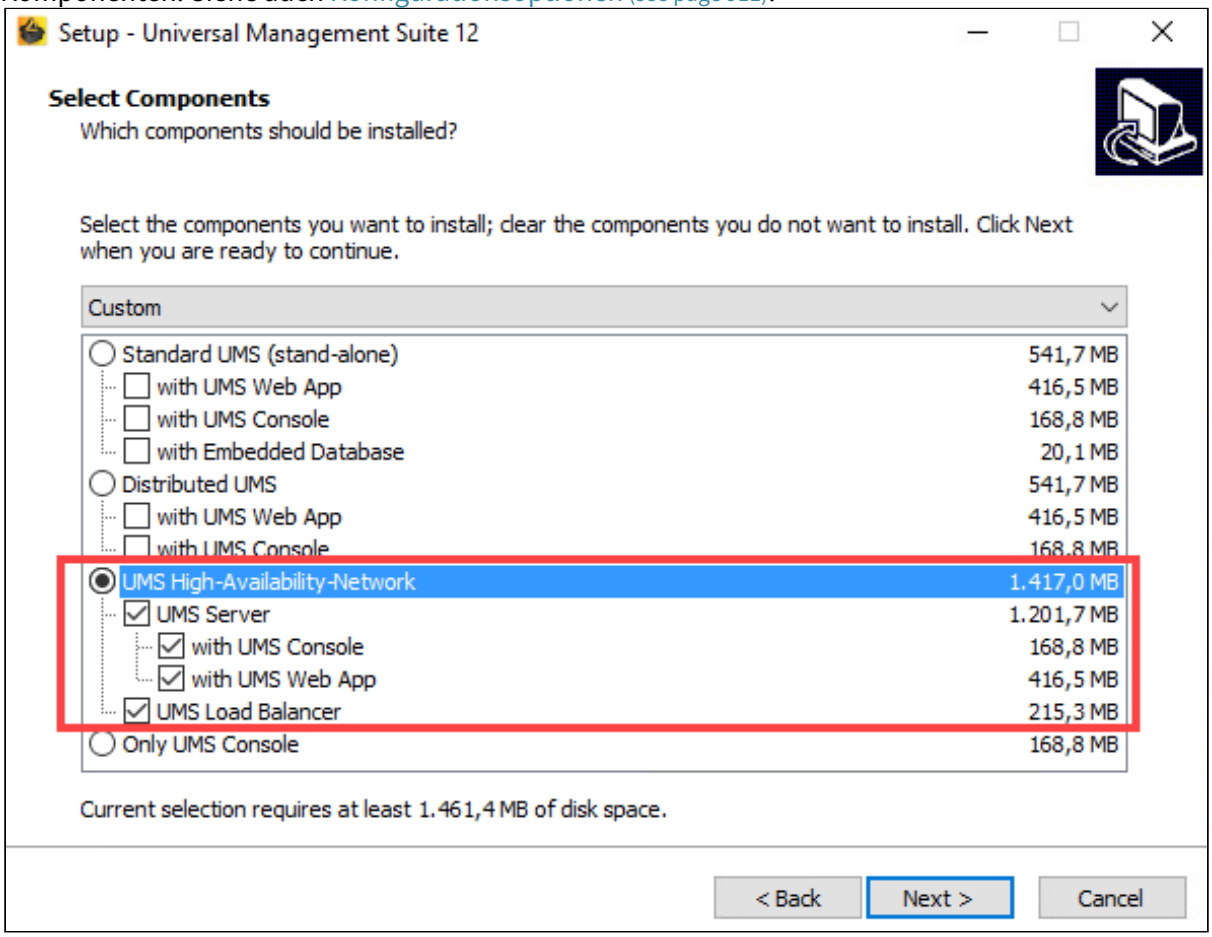
▶ Starten Sie den `IGEL RMGUIServer` -Dienst neu (für die Anleitung siehe IGEL UMS HA-Dienste und -Prozesse (see page 949)) und verwenden Sie in diesem Fall das Netzwerktoken, das beim Start des UMS Servers erzeugt wird, aus dem Verzeichnis:
Windows: `C:\Windows\System32\config\systemprofile\IGEL-Network.token`
Linux: `/root/IGEL-Network.token`

Die Installation starten

1. Starten Sie den UMS Installer.

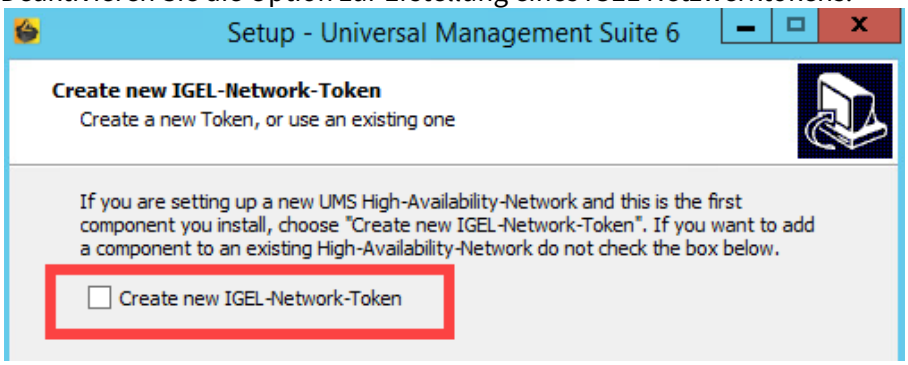
Sie benötigen Administrationsrechte, um IGEL UMS HA installieren zu können.

2. Lesen und bestätigen Sie die Lizenzvereinbarung unter **License Agreement**.
3. Lesen Sie die **Information** über den Installationsprozess.
4. Wählen Sie einen Pfad für die Installation.
5. Wählen Sie je nach Ihrer gewünschten HA-Netzwerkkonfiguration die zu installierenden Komponenten. Siehe auch Konfigurationsoptionen (see page 911).

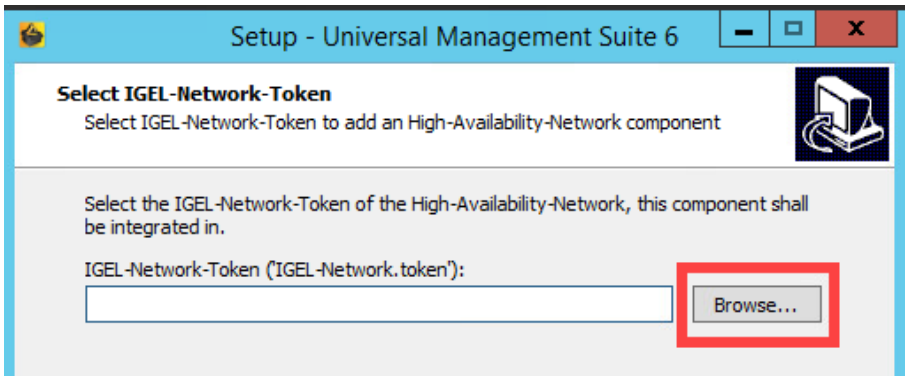


6. Bestätigen Sie den Dialog, dass Ihr System die angezeigten Systemanforderungen erfüllt.
7. Wählen Sie unter **UMS data directory** das Verzeichnis, in dem Universal Firmware Updates und Dateien gespeichert werden sollen.

8. Deaktivieren Sie die Option zur Erstellung eines IGEL Netzwerktokens.



9. Wählen Sie das zu verwendende IGEL Netzwerktoken aus.



10. Wenn die interne Windows Firewall auf dem Hostrechner aktiv ist: Überprüfen Sie die Einstellungen unter **Windows firewall settings** und ändern Sie diese, falls nötig. Jeder Port, der hier aktiviert ist, wird in der Windows Firewall auf dem Hostrechner des UMS Servers als Regel definiert.

> **UMS 12 Kommunikationsports**
> Wenn Sie Änderungen am Netzwerk vornehmen möchten, sollten Sie die folgenden Ports und Pfade berücksichtigen:
> - Für IGEL OS 12-Geräte ist TCP 8443 /device-connector/* erforderlich.
>   SSL kann am Reverse Proxy / externen Load Balancer (siehe IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading) oder am UMS Server terminiert werden.
> - Für den Import von IGEL OS 12 Apps vom IGEL App Portal in die UMS ist die URL https://app.igel.com/ (TCP 443) erforderlich.
> - Für die UMS Web App sind TCP 8443 /webapp/* und /wums-app/* erforderlich.
> - Für die UMS Konsole ist der Root erforderlich, d. h. TCP 8443 /*
> - Für IGEL OS 11-Geräte sind TCP 30001 und TCP/UDP 30005 erforderlich.
>
> Weitere Informationen zu UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).

11. Geben Sie unter **Select Start Menu Folder** einen Ordnernamen für die Verknüpfung an.

12. Wählen Sie unter **Select Additional Tasks**, ob Sie auf dem Desktop Verknüpfungen für UMS Konsole und UMS Administrator anlegen möchten.
13. Lesen Sie die Zusammenfassung und starten Sie den Installationsprozess.
14. Schließen Sie den UMS Installer nach Abschluss der Installation.

Wenn Sie der Installation einen UMS Server hinzugefügt haben, erstellt der UMS Installer Einträge im Windows-Softwareverzeichnis und im Startmenü. Die Anwendungen UMS Konsole und UMS Administrator werden installiert, und, falls dies ausgewählt wurde, werden ihre Verknüpfungen auf dem Desktop abgelegt.

Fall Sie einen Load Balancer einzeln installiert haben, wird lediglich die Option zur Deinstallation der UMS im Windows-Startmenü angelegt. Am Load Balancer ist keine Konfiguration nötig. Er verbindet sich beim Starten selbstständig mit dem HA-Netzwerk.

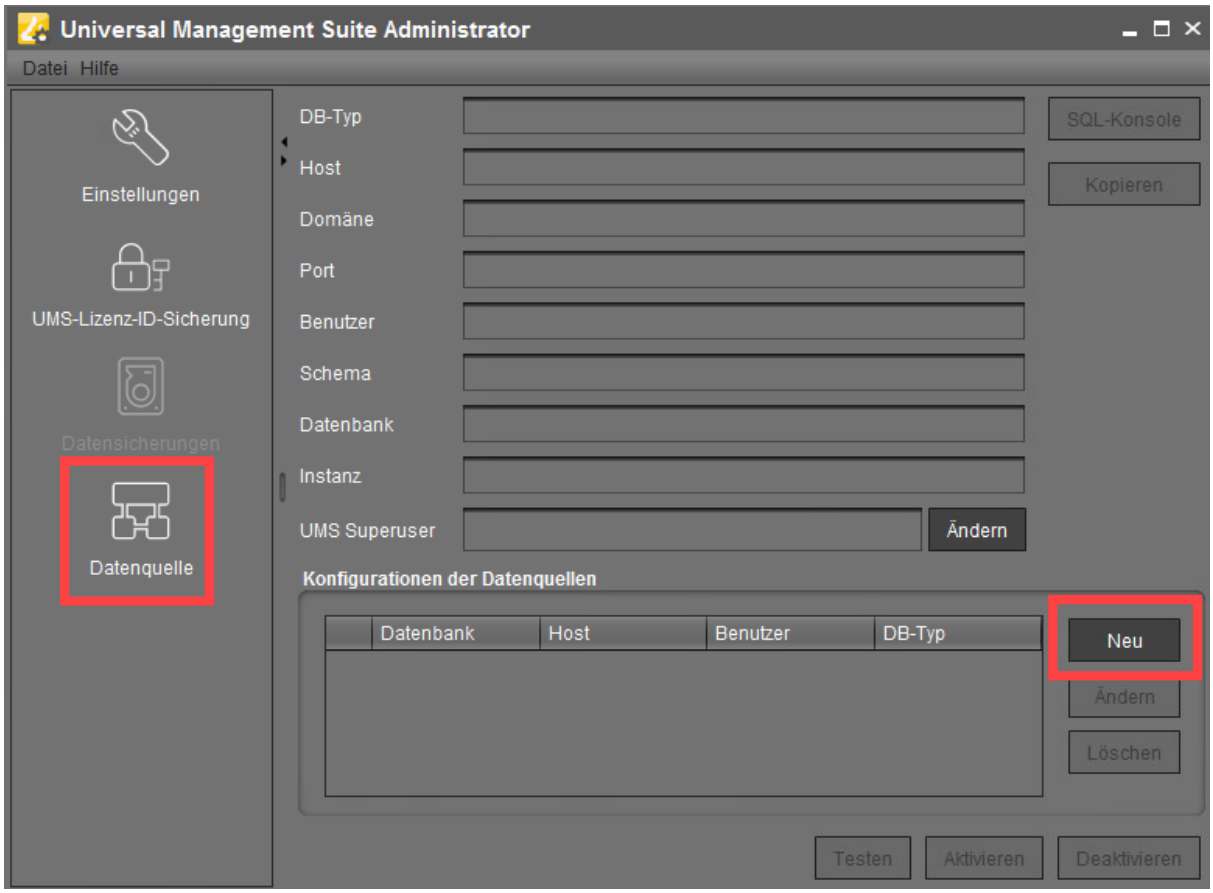
> Wird SQL Server AD nativ (see page 924) verwendet, müssen Sie auch den richtigen Starttyp und die richtigen Anmeldedaten für den Dienst "IGEL RMGUIServer" einstellen und den Dienst neu starten. Dies muss auf **ALLEN** UMS Server-Hosts durchgeführt werden. Für Details siehe "Windows-Dienst für UMS Server konfigurieren" unter "UMS für SQL Server AD nativ einrichten" (see page 924).

Die Installation überprüfen

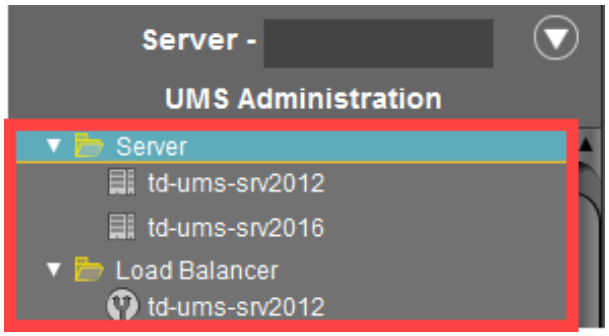
1. Prüfen Sie, ob alle Prozesse laufen. Die Liste der Prozesse für UMS HA finden Sie unter IGEL UMS HA-Dienste und -Prozesse (see page 949).
2. Falls Sie den UMS Server einer Installation hinzugefügt haben, gehen Sie auf **UMS Administrator > Datenquelle** und überprüfen Sie, ob die Datenbankverbindung erfolgreich vom bereits laufenden UMS Server übertragen wurde.

   > Standardpfad zum UMS Administrator:
   > Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
   > Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
   > Die Anwendung IGEL UMS Administrator kann nur auf dem UMS Server gestartet werden.

   Wenn die Datenbankverbindung nicht automatisch eingerichtet wurde, geben Sie unter **UMS Administrator > Datenquelle > Neu** genau die gleichen Datenbankparameter ein, die Sie bei der Installation des ersten HA-Servers (see page 921) verwendet haben, und klicken Sie auf **Aktivieren**.



3. Gehen Sie in der UMS Konsole auf **UMS Administration > UMS Netzwerk** und überprüfen Sie die Knoten **Server** und **Load Balancer**.



Außerdem können Sie die Funktion zur Überprüfung der HA-Installation verwenden, siehe UMS HA Statusprüfung - Ihre High Availability- und Distributed UMS-Systeme analysieren (see page 944).

Um IGEL OS 12-Geräte zu verwalten, müssen Sie Ihre UMS nach der Installation registrieren, siehe IGEL UMS registrieren (see page 321).

Für die Zukunft können auch die folgenden Artikel nützlich sein: Ein Backup der IGEL UMS erstellen (see page 720) und Welche Dateien werden automatisch zwischen den IGEL UMS Servern synchronisiert? (see page 151).

Installation eines HA-Netzwerks aktualisieren

Anwendungsfall

Sie haben bereits eine UMS HA-Installation (High Availability) (see page 909) und müssen diese aktualisieren.

Allgemeiner Überblick

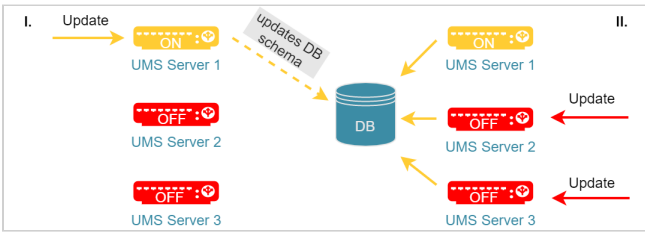
Es gibt zwei mögliche Verfahren zum HA-Update:

- mit kurzer Ausfallzeit der Server (see page 931) (empfohlen)
- ohne Ausfallzeit der Server, aber mit automatischem Kopieren der produktiven Datenbank in eine temporäre Datenbank, (see page 932) was in der Regel zu einer längeren Aktualisierungszeit führt

Mit kurzer Ausfallzeit

In diesem Fall sieht der Aktualisierungsvorgang allgemein wie folgt aus:

1. Stoppen Sie alle UMS Server bis auf einen (überprüfen Sie dies in der Serverliste der UMS Konsole, die mit dem letzten laufenden Server verbunden ist).
2. Aktualisieren Sie diesen UMS Server. Sobald das Update abgeschlossen ist, wird die produktive Datenbank beim Starten des Servers aktualisiert.
3. Aktualisieren Sie die übrigen UMS Server (parallel oder nacheinander). Sobald das Update abgeschlossen ist, verbinden sie sich automatisch mit der produktiven Datenbank.
4. Aktualisieren Sie andere Komponenten wie separate UMS Load Balancer und/oder UMS Konsolen.



Detaillierte Anweisungen finden Sie unter HA-Installation aktualisieren: Mit Ausfallzeit der Server (see page 933).

⚠ IGEL empfiehlt diese Methode für das HA-Update aufgrund einer Reihe von Vorteilen:

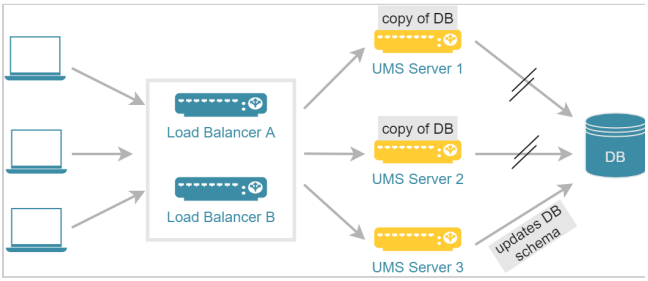
- Der Aktualisierungsvorgang ist wesentlich schneller.
- Keine Datenbankinkonsistenzen, da während des Updates keine anderen Server und Prozesse die Datenbank nutzen.

- Nur kurze Ausfallzeit. Hinweis: Da es keine Kommunikation zwischen den Servern und Geräten gibt (während der Aktualisierung des ersten UMS Servers), können keine benutzerspezifischen Profile bereitgestellt werden (IGEL Shared Workplace).

Ohne Ausfallzeit

In diesem Fall sieht der Aktualisierungsvorgang allgemein wie folgt aus:

1. Aktualisieren Sie alle UMS Server auf eine neue Version, ein Server nach dem anderen.
   Während der Aktualisierung trennt sich ein UMS Server von der produktiven Datenbank und speichert eine Kopie davon lokal in einer eingebetteten Derby-Datenbank. Die Kopie wird für jeden Server erstellt, außer für den letzten. Der zuletzt aktualisierte UMS Server aktualisiert auch das Schema der produktiven Datenbank. Danach verbinden sich alle anderen UMS Server wieder mit der ursprünglichen produktiven Datenbank.
2. Aktualisieren Sie andere Komponenten wie separate UMS Load Balancer und/oder UMS Konsolen.



Detaillierte Anweisungen finden Sie unter HA-Installation aktualisieren: Ohne Ausfallzeit der Server (see page 938).

⚠ Bei dieser Aktualisierungsmethode können alle UMS Server während des Aktualisierungsprozesses jederzeit von den Endgeräten angesprochen werden, z. B. um benutzerspezifische Profile bereitzustellen (IGEL Shared Workplace). Beachten Sie jedoch das Folgende:

- Das Kopieren der Daten von der produktiven Datenbank in die temporäre Datenbank kann sehr viel Zeit in Anspruch nehmen.
- Anfragen von Geräten können den Kopiervorgang beeinträchtigen.
- Änderungen in der temporären Datenbank gehen verloren, sobald die Server nach Abschluss der Aktualisierung wieder auf die produktive Datenbank umschalten.

- HA-Installation aktualisieren: Mit Ausfallzeit der Server (see page 933)
- HA-Installation aktualisieren: Ohne Ausfallzeit der Server (see page 938)

HA-Installation aktualisieren: Mit Ausfallzeit der Server

Einen Kurzüberblick über das Aktualisierungsverfahren von High Availability (HA) finden Sie unter Installation eines HA-Netzwerks aktualisieren (see page 931).

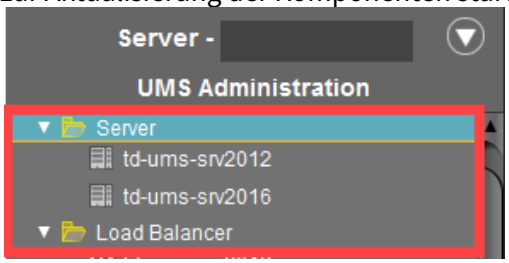
Um die HA-Installation zu aktualisieren, folgen Sie diesen Anweisungen in der angegebenen Reihenfolge.

Update vorbereiten

Führen Sie die folgenden Schritte aus, bevor Sie einen Server aktualisieren:

1. Laden Sie die aktuelle Version der IGEL Universal Management Suite vom IGEL Downloadserver[41] herunter und verteilen Sie die Installationsdatei auf alle Systeme mit UMS Komponenten (UMS Server, UMS Load Balancer, UMS Konsolen).

2. Rufen Sie die Liste der UMS Server und Load Balancer im HA-Netzwerk in der UMS Konsole > **UMS Administration > UMS Netzwerk** auf und überprüfen Sie, ob die aufgeführten Komponenten tatsächlich im Netzwerk vorhanden sind. Löschen Sie verwaiste Einträge, bevor Sie den Prozess zur Aktualisierung der Komponenten starten.



3. Erstellen Sie ein Backup Ihrer Datenbank, bevor Sie mit der Update-Installation beginnen. Verwenden Sie die vom DBMS-Hersteller vorgesehene Vorgehensweise zu Backup. Siehe auch Ein Backup der IGEL UMS erstellen (see page 720).

   Warnung

   Es ist nicht möglich, eine UMS Version zu installieren, die älter ist als die aktuelle. Wenn Sie auf eine ältere Version (z.B von 6.10 auf 6.09) wechseln möchten, müssen Sie ein separates HA-Netzwerk installieren und eine Datenbanksicherung des entsprechenden Schemas wiederherstellen. Dies ist auch einer der Gründe, warum Sie das laufende System sichern sollten, bevor Sie das UMS HA-Netzwerk aktualisieren.
   Da die Version des Datenbankschemas immer der aktuellen Major.Minor-Version der UMS entspricht (d.h. 6.10 für alle 6.10.x-Releases, 6.08 für alle 6.08.x-Releases), sind Downgrades nur innerhalb einer Major.Minor-Version möglich. Beispiel: Sie können ein Downgrade von 6.10.140 auf 6.10.120 durchführen, aber nicht von 6.10.140 auf 6.09.120.

4. Überprüfen Sie, ob die Zeit auf allen Servern synchronisiert ist.

41 https://www.igel.com/software-downloads/

> ⚠ Um Probleme mit Ihrer HA-Installation zu vermeiden, stellen Sie sicher, dass der Zeitunterschied auf den Servern des HA-Netzwerks eine Minute nicht überschreitet. Nach jeder manuellen Zeitänderung müssen die HA-Dienste auf dem entsprechenden Server neu gestartet werden.

UMS Server aktualisieren

Das Hauptmerkmal dieser Aktualisierungsmethode ist, dass am Anfang geprüft wird, wie viele UMS Server "online" sind. Wenn aktiv nur einer ist, auf dem das Update gestartet wurde, wird keine temporäre Datenbank mit einer Kopie der produktiven Datenbank erstellt und die produktive Datenbank wird sofort aktualisiert, d. h. sobald der UMS Server nach Abschluss des Updates startet. Daher ist es notwendig, NUR EINEN UMS Server laufen zu lassen, nämlich den, mit dem Sie den Updatevorgang starten. Dies kann ein beliebiger UMS Server innerhalb Ihres HA-Netzwerks sein.

1. Stoppen Sie alle UMS Server außer dem einen, auf dem Sie das Update starten wollen. Sie können UMS Server in der UMS Konsole unter **UMS Administration > UMS Netzwerk > Server > [Servername] > Dienst anhalten** oder in den Windows-Diensten stoppen, siehe IGEL UMS HA-Dienste und -Prozesse (see page 949).

2. Stellen Sie sicher, dass nur ein UMS Server läuft und die anderen gestoppt sind:
   - durch Überprüfung der Server-Liste in der UMS Konsole unter **UMS Administration > UMS Netzwerk > Server**
     ODER
   - mit der folgenden SQL-Anweisung:

```
select
        ep.epr_process_id,
        ep.epr_process_host,
        ep.epr_process_mode,
        ep.epr_service_status
from
        epr_processes ep
where
        ep.epr_process_type = 'UMS_RMGUISERVER'
```

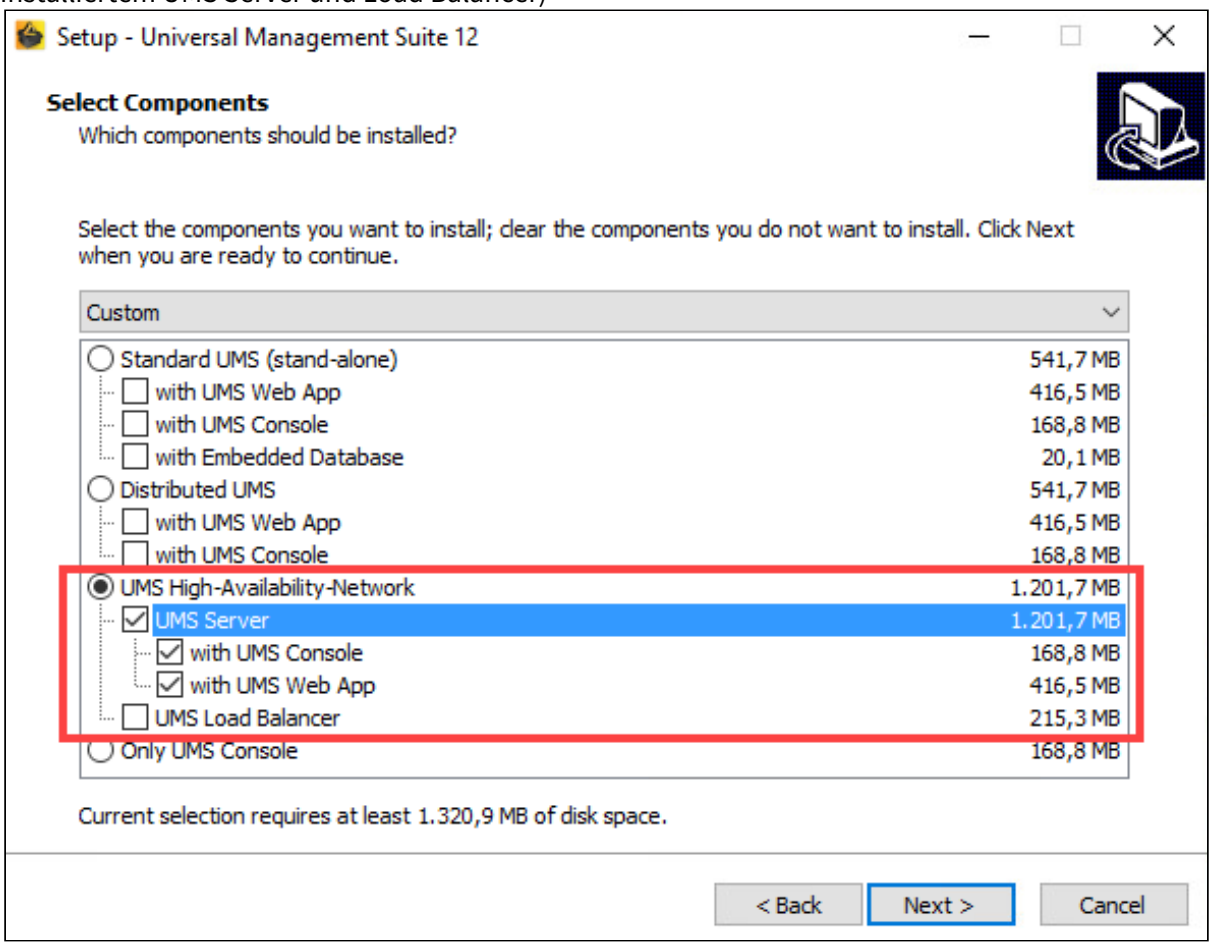
     `SERVICE_RUNNING` muss nur für den Server angezeigt werden, den Sie gerade aktualisieren wollen.
     `SERVICE_STOPPED` muss für alle anderen Server angezeigt werden.

3. Starten Sie den UMS Installer.

> ⓘ Für die Aktualisierung von IGEL UMS HA benötigen Sie Administratorrechte.

⚠ Wenn der UMS Server als Teil des HA-Netzwerks unter Linux installiert wird, muss das Verzeichnis `/root` für den Benutzer `root` schreibbar sein.

4. Lesen und bestätigen Sie die Lizenzvereinbarung unter **License Agreement**.
5. Lesen Sie die **Information** über den Installationsprozess.
6. Überprüfen Sie die zu installierenden Komponenten. (In diesem Beispiel: HA-Netzwerk mit einzeln installiertem UMS Server und Load Balancer)



7. Bestätigen Sie den Dialog, dass Ihr System die angezeigten Systemanforderungen erfüllt.
8. Wählen Sie unter **Select Additional Tasks**, ob Sie auf dem Desktop Verknüpfungen für UMS Konsole und UMS Administrator anlegen möchten.
9. Wenn die interne Windows Firewall auf dem Hostrechner aktiv ist: Überprüfen Sie die Einstellungen unter **Windows firewall settings** und ändern Sie diese, falls nötig. Jeder Port, der

hier aktiviert ist, wird in der Windows Firewall auf dem Hostrechner des UMS Servers als Regel definiert.

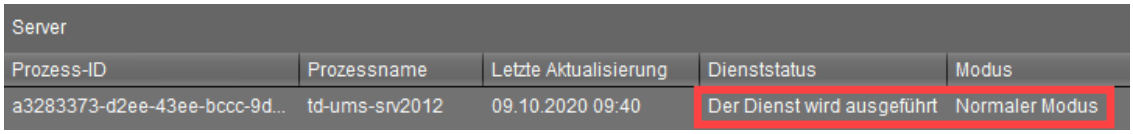
> **UMS 12 Kommunikationsports**
> Wenn Sie Änderungen am Netzwerk vornehmen möchten, sollten Sie die folgenden Ports und Pfade berücksichtigen:
> - Für IGEL OS 12-Geräte ist TCP 8443 /device-connector/* erforderlich.
>   SSL kann am Reverse Proxy / externen Load Balancer (siehe IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading) oder am UMS Server terminiert werden.
> - Für den Import von IGEL OS 12 Apps vom IGEL App Portal in die UMS ist die URL https://app.igel.com/ (TCP 443) erforderlich.
> - Für die UMS Web App sind TCP 8443 /webapp/* und /wums-app/* erforderlich.
> - Für die UMS Konsole ist der Root erforderlich, d. h. TCP 8443 /*
> - Für IGEL OS 11-Geräte sind TCP 30001 und TCP/UDP 30005 erforderlich.
>
> Weitere Informationen zu UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).

10. Lesen Sie die Zusammenfassung und starten Sie den Installationsprozess.

11. Schließen Sie den UMS Installer nach Abschluss der Installation.
    Der UMS Server wird gestartet und aktualisiert die Datenbank.

> Wird SQL Server AD nativ (see page 933) verwendet, müssen Sie auch den richtigen Starttyp und die richtigen Anmeldedaten für den Dienst "IGEL RMGUIServer" einstellen und den Dienst neu starten. Dies muss auf **ALLEN** UMS Server-Hosts durchgeführt werden. Für Details siehe "Windows-Dienst für UMS Server konfigurieren" unter "UMS für SQL Server AD nativ einrichten" (see page 933).

12. Öffnen Sie die UMS Konsole und gehen Sie auf **UMS Administration > UMS Netzwerk > Server**, um zu überprüfen, ob der Server
    - erfolgreich aktuallisiert ist
    - läuft
    - im normalen Modus ist



13. Aktualisieren Sie die übrigen UMS Server, entweder parallel oder nacheinander, indem Sie die Schritte 3-11 wiederholen.
    Nach dem Update starten die Server automatisch und verbinden sich mit der produktiven Datenbank.

Weitere Komponenten aktualisierien

Nach der Aktualisierung der UMS Server im HA-Netzwerk müssen Sie alle anderen aktuellen UMS Komponenten, wie z. B. separate UMS Load Balancer und UMS Konsolen, aktualisieren.

1. Führen Sie dazu den UMS Installer auf den Systemen aus.

2. Überprüfen Sie die zu installierenden Komponenten.

   > Sie können sich nicht mit dem UMS Server mit einer Konsolenversion verbinden, die älter ist als die Version des UMS Servers.

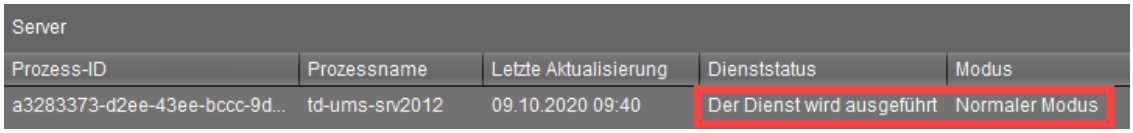
   > Load Balancer sind in der Lage, mit UMS Servern neuerer Versionen zu interagieren, sollten aber für eine optimale Leistung die gleiche Version wie die UMS Server haben.

Siehe auch Load Balancer stoppt nicht während der Aktualisierung der HA-Installation (see page 150).

Die Installation überprüfen

1. Prüfen Sie, ob alle Prozesse laufen. Die Liste der Prozesse für UMS HA finden Sie unter IGEL UMS HA-Dienste und -Prozesse (see page 949).

2. Gehen Sie in der UMS Konsole auf **UMS Administration > UMS Netzwerk** und überprüfen Sie die Knoten **Server** und **Load Balancer**.
   Alle Server und Load Balancer müssen
   - aktuallisiert sein
   - laufen
   - im normalen Modus sein



HA-Installation aktualisieren: Ohne Ausfallzeit der Server

⚠ Vor der Aktualisierung lesen Sie Installation eines HA-Netzwerks aktualisieren (see page 931).

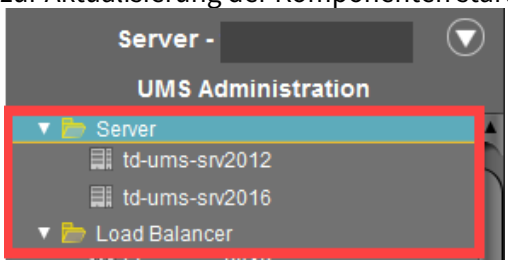
Um die HA-Installation zu aktualisieren, folgen Sie diesen Anweisungen in der angegebenen Reihenfolge.

Update vorbereiten

Führen Sie die folgenden Schritte aus, bevor Sie einen Server aktualisieren:

1. Laden Sie die aktuelle Version der IGEL Universal Management Suite vom IGEL Downloadserver[42] herunter und verteilen Sie die Installationsdatei auf alle Systeme mit UMS Komponenten (UMS Server, UMS Load Balancer, UMS Konsolen).

2. Rufen Sie die Liste der UMS Server und Load Balancer im HA-Netzwerk in der UMS Konsole > **UMS Administration > UMS Netzwerk** auf und überprüfen Sie, ob die aufgeführten Komponenten tatsächlich im Netzwerk vorhanden sind. Löschen Sie verwaiste Einträge, bevor Sie den Prozess zur Aktualisierung der Komponenten starten.



3. Erstellen Sie ein Backup Ihrer Datenbank, bevor Sie mit der Update-Installation beginnen. Verwenden Sie die vom DBMS-Hersteller vorgesehene Vorgehensweise zu Backup. Siehe auch Ein Backup der IGEL UMS erstellen (see page 720).

   Warnung

   Es ist nicht möglich, eine UMS Version zu installieren, die älter ist als die aktuelle. Wenn Sie auf eine ältere Version (z.B. von 6.10 auf 6.09) wechseln möchten, müssen Sie ein separates HA-Netzwerk installieren und eine Datenbanksicherung des entsprechenden Schemas wiederherstellen. Dies ist auch einer der Gründe, warum Sie das laufende System sichern sollten, bevor Sie das UMS HA-Netzwerk aktualisieren.
   Da die Version des Datenbankschemas immer der aktuellen Major.Minor-Version der UMS entspricht (d.h. 6.10 für alle 6.10.x-Releases, 6.08 für alle 6.08.x-Releases), sind Downgrades nur innerhalb einer Major.Minor-Version möglich. Beispiel: Sie können ein Downgrade von 6.10.140 auf 6.10.120 durchführen, aber nicht von 6.10.140 auf 6.09.120.

4. Überprüfen Sie, ob die Zeit auf allen Servern synchronisiert ist.

42 https://www.igel.com/software-downloads/

> ⚠ Um Probleme mit Ihrer HA-Installation zu vermeiden, stellen Sie sicher, dass der Zeitunterschied auf den Servern des HA-Netzwerks eine Minute nicht überschreitet. Nach jeder manuellen Zeitänderung müssen die HA-Dienste auf dem entsprechenden Server neu gestartet werden.

UMS Server aktualisieren

Im Updatemodus laufen die UMS Server mit einer lokalen Kopie der Datenbank. Dadurch wird sichergestellt, dass sie Anfragen der Geräte beantworten und Konfigurationseinstellungen und Profile auf die Geräte übertragen können.

> ⚠ Im Updatemodus können Sie sich mit den Servern über die UMS Konsole verbinden. Alle Änderungen, die in dieser Zeit in der UMS Konsole vorgenommen wurden, gehen nach dem Update verloren.

> **Warnung**
>
> Nehmen Sie während des Aktualisierungsvorgangs keine Änderungen an der produktiven Datenbank vor. Denn entkoppelte Server arbeiten in der Zwischenzeit mit einer Kopie des Datenbankschemas. Aus diesem Grund sollte das Update aller Komponenten innerhalb des UMS HA-Netzwerks sofort durchgeführt werden. Implementieren Sie ein Testsystem für die Erstinstallation neuer IGEL UMS Versionen und überprüfen Sie deren Prozesse, bevor Sie sie in das Produktivsystem übertragen. Dies gilt auch für Hotfixes, Patches usw. für Serversysteme und Datenbanken.

Die ersten UMS Server aktualisieren

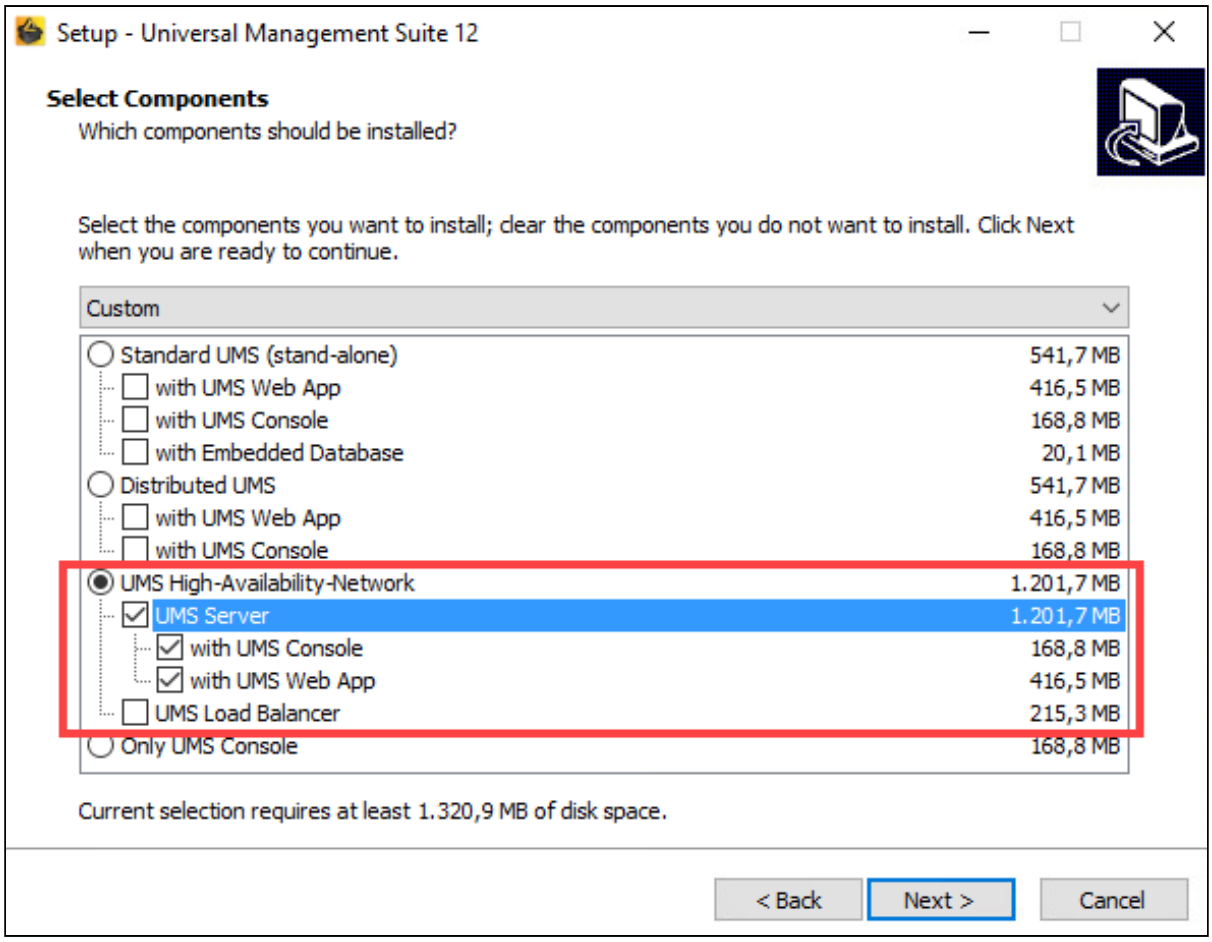
Sie können einen beliebigen UMS Server im HA-Netzwerk auswählen, um den Aktualisierungsvorgang zu starten.

1. Starten Sie den UMS Installer.

   > ⓘ Für die Aktualisierung von IGEL UMS HA benötigen Sie Administratorrechte.

   > ⚠ Wenn der UMS Server als Teil des HA-Netzwerks unter Linux installiert wird, muss das Verzeichnis `/root` für den Benutzer `root` schreibbar sein.

2. Lesen und bestätigen Sie die Lizenzvereinbarung unter **License Agreement**.
3. Lesen Sie die **Information** über den Installationsprozess.
4. Überprüfen Sie die zu installierenden Komponenten. (In diesem Fall: HA-Netzwerk mit einzeln installiertem UMS Server und Load Balancer)



5. Bestätigen Sie den Dialog, dass Ihr System die angezeigten Systemanforderungen erfüllt.

6. Wählen Sie unter **Select Additional Tasks**, ob Sie auf dem Desktop Verknüpfungen für UMS Konsole und UMS Administrator anlegen möchten.

7. Wenn die interne Windows Firewall auf dem Hostrechner aktiv ist: Überprüfen Sie die Einstellungen unter **Windows firewall settings** und ändern Sie diese, falls nötig. Jeder Port, der hier aktiviert ist, wird in der Windows Firewall auf dem Hostrechner des UMS Servers als Regel definiert.

   UMS 12 Kommunikationsports
   Wenn Sie Änderungen am Netzwerk vornehmen möchten, sollten Sie die folgenden Ports und Pfade berücksichtigen:
   - Für IGEL OS 12-Geräte ist TCP 8443 /device-connector/* erforderlich.
     SSL kann am Reverse Proxy / externen Load Balancer (siehe IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading) oder am UMS Server terminiert werden.

- Für den Import von IGEL OS 12 Apps vom IGEL App Portal in die UMS ist die URL https://app.igel.com/ (TCP 443) erforderlich.
- Für die UMS Web App sind TCP 8443 /webapp/* und /wums-app/* erforderlich.
- Für die UMS Konsole ist der Root erforderlich, d. h. TCP 8443 /*
- Für IGEL OS 11-Geräte sind TCP 30001 und TCP/UDP 30005 erforderlich.

Weitere Informationen zu UMS Ports finden Sie unter IGEL UMS Kommunikationsports (see page 6).

8. Lesen Sie die Zusammenfassung und starten Sie den Installationsprozess.
   Während der Installation wechselt der UMS Server in den Updatemodus.

9. Bestätigen Sie die Meldung `n of m servers updated`.
   Beispiel:

10. Schließen Sie den UMS Installer nach Abschluss der Installation.

    Wird SQL Server AD nativ (see page 938) verwendet, müssen Sie auch den richtigen Starttyp und die richtigen Anmeldedaten für den Dienst "IGEL RMGUIServer" einstellen und den Dienst neu starten. Dies muss auf **ALLEN** UMS Server-Hosts durchgeführt werden. Für Details siehe "Windows-Dienst für UMS Server konfigurieren" unter "UMS für SQL Server AD nativ einrichten" (see page 938).

11. Fahren Sie mit dem Update des nächsten UMS Servers fort.

Den letzten UMS Server aktualisieren

▶ Wiederholen Sie die Schritte 1-9 (see page 939) für den letzten UMS Server, der aktualisiert werden soll.

Der letzte UMS Server, der aktualisiert wird, erneuert nach der Installation das Schema der produktiven Datenbank. Alle anderen UMS Server im Netzwerk, die im Updatemodus laufen, werden darüber informiert, dass die Installation abgeschlossen ist. Sie werden neu starten und sich wieder mit der produktiven Datenbank verbinden. Anschließend laufen sie im normalen Modus.

Weitere Komponenten aktualisierien

Nach der Aktualisierung der UMS Server im HA-Netzwerk müssen Sie alle anderen aktuellen UMS Komponenten, wie z. B. separate UMS Load Balancer und UMS Konsolen aktualisieren.

1. Führen Sie dazu den UMS Installer auf den Systemen aus.

2. Überprüfen Sie die zu installierenden Komponenten.

   > Sie können sich nicht mit dem UMS Server mit einer Konsolenversion verbinden, die älter ist als die Version des UMS Servers.

   > Load Balancer sind in der Lage, mit UMS Servern neuerer Versionen zu interagieren, sollten aber für eine optimale Leistung die gleiche Version wie die UMS Server haben.

Siehe auch Load Balancer stoppt nicht während der Aktualisierung der HA-Installation (see page 150).

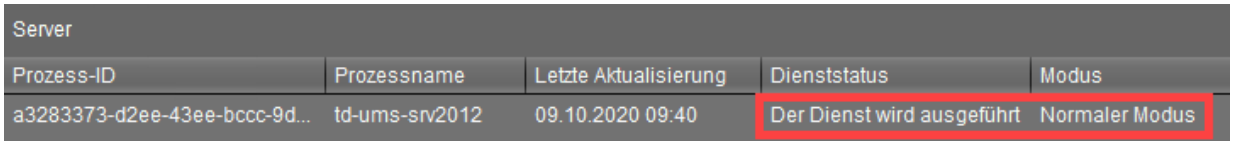
Die Installation überprüfen

1. Prüfen Sie, ob alle Prozesse laufen. Die Liste der Prozesse für UMS HA finden Sie unter IGEL UMS HA-Dienste und -Prozesse (see page 949).

2. Gehen Sie im UMS Administrator (see page 707) auf **Datenquelle**, um zu überprüfen, ob die Datenbank aktiviert ist.

   > ⚠ Wenn die Serverliste zu Beginn des Updates nicht überprüft wurde (siehe Update vorbereiten (see page 938), Schritt 2) und mehr Server in der Datenbank registriert waren, als tatsächlich laufen, kann es sein, dass es einen Server im HA-Netzwerk gibt, der sich nicht wieder mit der produktiven Datenbank verbunden hat.
   > In diesem Fall wechseln Sie die Datenquelle manuell in die produktive Datenbank. Alternativ können Sie dafür im UMS Administrator > Distributed UMS (see page 738) die Schaltfläche **Update-Modus von lokalem UMS Server beenden** verwenden.
   > Das Datenbankschema wird bei der ersten Verbindung eines aktualisierten Servers mit der produktiven Datenbank erneuert. Anschließend können alle anderen Server im Netzwerk auf diese Datenbank umgestellt werden.

3. Gehen Sie in der UMS Konsole auf **UMS Administration > UMS Netzwerk** und überprüfen Sie die Knoten **Server** und **Load Balancer**.
   Alle Server und Load Balancer müssen
   - aktuallisiert sein
   - laufen
   - im normalen Modus sein



Lizenzierung der High-Availability-Erweiterung

IGEL OS 11 und höher

Die IGEL UMS High-Availability-Erweiterung braucht keine zusätzliche Lizenz.

Vor IGEL OS 11

Die High-Availability-Erweiterung ist in Paketen von jeweils 50 Lizenzen erhältlich. Diese Lizenzen werden in der UMS installiert. Die UMS prüft, ob die Anzahl der Lizenzen mindestens so hoch ist wie die Anzahl der Geräte, die mit der UMS verbunden sind.

Jede Version der IGEL UMS enthält fünf Testlizenzen, die Ihnen ermöglichen, die Funktion kostenlos und ohne Registrierung zu evaluieren.

▶ Registrieren Sie die Lizenzdatei in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Lizenzen > UMS Lizenzen**.

> Ein HA-Netzwerk funktioniert nur mit einer Lizenz, die alle verwalteten Geräte abdeckt, die in der UMS registriert sind. Ein Mischbetrieb (Geräte mit HA-Unterstützung und Geräte ohne HA-Unterstützung) ist nicht möglich.

UMS HA Statusprüfung - Ihre High Availability- und Distributed UMS-Systeme analysieren

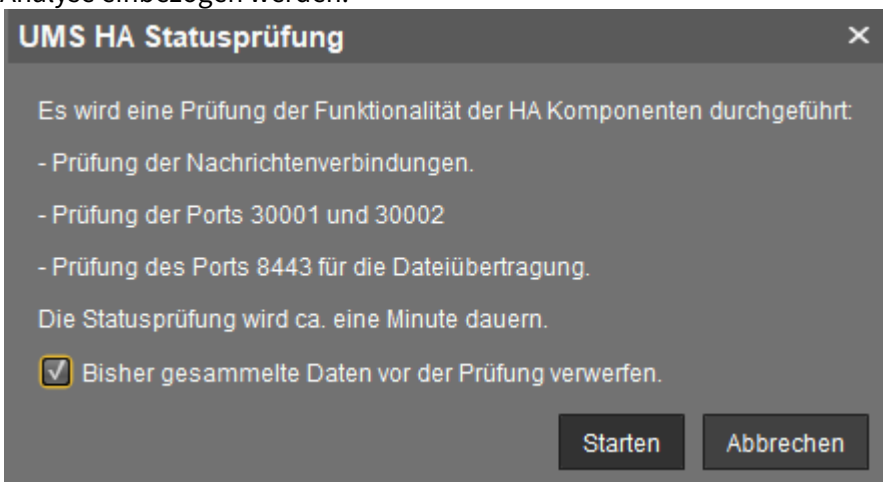
Mit der Funktion **UMS HA Statusprüfung** können Sie eine Gesamtprüfung Ihrer IGEL Universal Management Suite (UMS) Multiinstanz-Installation (see page 246) durchführen. Dabei wird geprüft, ob die Interaktion zwischen den Komponenten des High Availability-Systems (HA) oder der Distributed UMS funktioniert, insbesondere ob die Komponenten Nachrichten und Daten austauschen können.

> ⓘ Die Berechtigung zur Verwendung der Funktion **UMS HA Statusprüfung** kann unter **System > Administratorkonten** eingestellt werden, siehe Allgemeine Administratorenrechte (see page 682).

Menüpfad: Menüleiste **> Hilfe > UMS HA Statusprüfung**

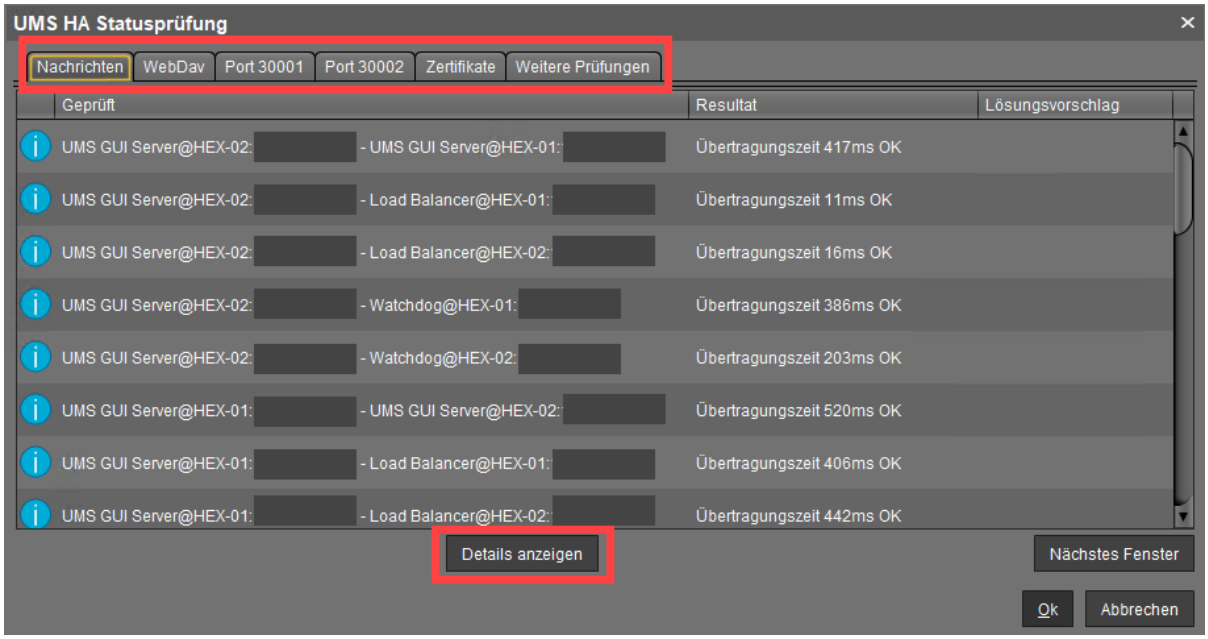
So können Sie Ihre HA-Umgebung / Distributed UMS überprüfen:

1. Stellen Sie sicher, dass sich die Server und die darauf installierten Komponenten im normalen Betriebsmodus befinden.
2. Gehen Sie in der Menüleiste auf **Hilfe > UMS HA Statusprüfung**.
3. Deaktivieren Sie das Kontrollkästchen **Bisher gesammelte Daten vor der Prüfung verwerfen**, wenn Sie möchten, dass die zwischengespeicherten Daten aus früheren Ausführungen in die Analyse einbezogen werden.



   Nachdem die erforderlichen Daten gesammelt und analysiert wurden, öffnet sich ein Fenster, in dem die Ergebnisse und die entsprechenden Lösungsvorschläge in einer Reihe von Registerkarten dargestellt werden. Jede Registerkarte hat eine Schaltfläche **Details anzeigen**, die einen detaillierten Analysebericht im HTML-Format öffnet. Die Beschreibung jeder Registerkarte und des

HTML-Berichts finden Sie weiter unten.

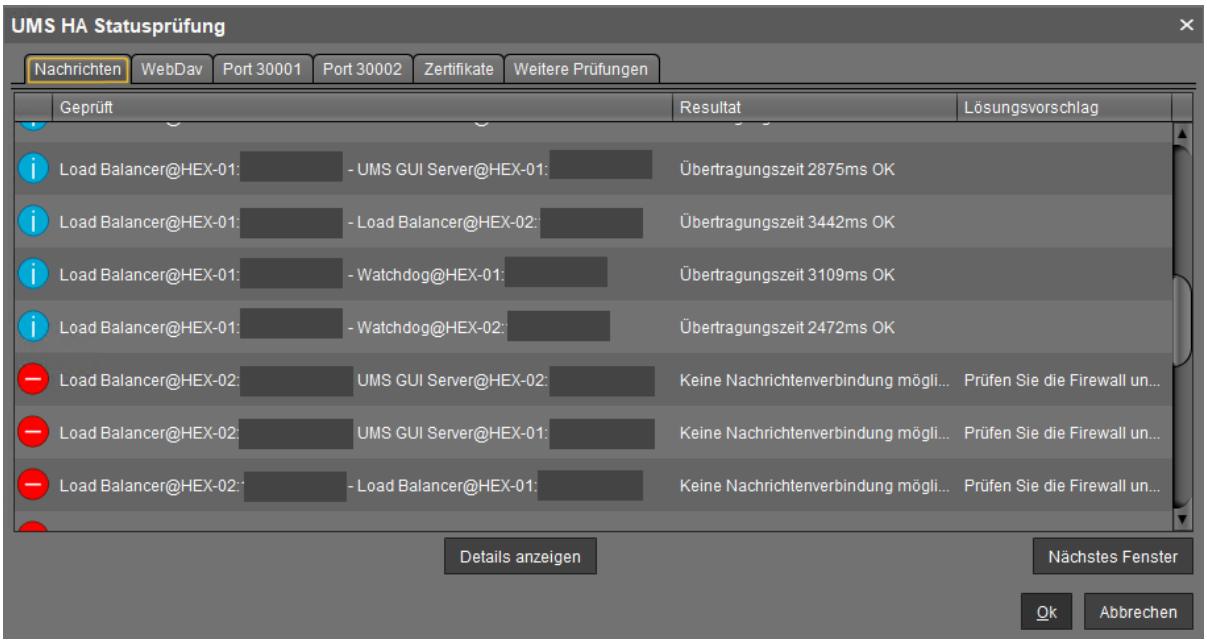


Nachrichten

Hier wird geprüft, ob die Komponenten laufen und Nachrichten austauschen können. Der Check führt einen Ping-Test zwischen den Komponenten der HA-Installation auf jedem Server durch. Die Liste zeigt das Ergebnis mit der Angabe der Übertragungszeit für jede Kombination der Komponenten. Die Übertragungszeit zeigt für die UMS HA an, ob das ActiveMQ Messaging innerhalb des Subnetzes funktioniert oder nicht.

Wenn Sie eine Distributed UMS-Installation haben, können die unter **Nachrichten** angezeigten Ergebnisse ignoriert werden, da die **UMS HA Statusprüfung** hauptsächlich die Leistung des ActiveMQ-Messaging der UMS High Availability (innerhalb des Subnetzes) überprüft. Für die Distributed UMS zeigt die Registerkarte **Nachrichten** die Nachrichtenverzögerung über die Datenbank an, die ca. 30 Sekunden beträgt.
Sie können derzeit auch das Folgende ignorieren:

- die **Nachrichten**-Ergebnisse des UMS HA Health Checks, wenn Ihre UMS HA ohne IGEL UMS Load Balancer in verschiedenen Subnetzen / Cloud-Umgebung installiert ist.
- Fehlermeldungen für Watchdogs, wenn Sie eine UMS HA ohne IGEL UMS Load Balancers haben



Die Gründe, warum der Nachrichtenaustausch zwischen Komponenten nicht möglich ist, sind in der Regel die folgenden:

- Eine der Komponenten läuft überhaupt nicht.
- Die erforderlichen Ports, 61616 und 6155, sind in der Firewall nicht offen. Siehe IGEL UMS Kommunikationsports (see page 6).
- Die Systemzeit auf den Servern ist sehr unterschiedlich.

  > ⚠ Um Probleme mit Ihrer HA-Installation zu vermeiden, stellen Sie sicher, dass der Zeitunterschied auf den Servern des HA-Netzwerks eine Minute nicht überschreitet. Nach jeder manuellen Zeitänderung müssen die HA-Dienste auf dem entsprechenden Server neu gestartet werden.

- Das IGEL Netzwerktoken ist nicht in allen Komponenten gleich. Dies kann beispielsweise daran liegen, dass bei der Installation weiterer UMS Server / UMS Load Balancer innerhalb eines HA-Netzwerks anstelle des Netzwerktokens, das ursprünglich bei der Installation des ersten UMS Servers erstellt wurde, ein neues IGEL Netzwerktoken generiert wird.

WebDav

Hier wird geprüft, ob die UMS Server Dateien über WebDav austauschen können. WebDav ist für die Synchronisierung von Dateien zwischen den UMS Servern zwingend erforderlich. Siehe auch Welche Dateien werden automatisch zwischen den IGEL UMS Servern synchronisiert? (see page 151).

Mögliche Gründe für das Scheitern sind die folgenden:

- Eine der Komponenten läuft überhaupt nicht.
- Der Port für WebDav 8443 ist in der Firewall nicht offen.

Port 30001

Port 30001 wird für Verbindungen zwischen den Geräten und dem UMS Load Balancer verwendet. Da der Test kein Gerät imitieren kann, versuchen die UMS Server, sich über Port 30001 mit dem UMS Load Balancer zu verbinden.

Mögliche Gründe für das Scheitern sind die folgenden:

- Eine der Komponenten läuft überhaupt nicht.
- Port 30001 ist in der Firewall nicht offen.

Port 30002

Port 30002 wird vom UMS Load Balancer für die Weiterleitung von Anfragen vom Gerät an den UMS Server verwendet.

Mögliche Gründe für das Scheitern sind die folgenden:

- Eine der Komponenten läuft überhaupt nicht.
- Port 30002 ist in der Firewall nicht offen.

Zertifikate

Hier werden die auf dem UMS Server gespeicherten Zertifikate mit den auf dem UMS Load Balancer gespeicherten Zertifikaten verglichen.

Ein möglicher Grund für das Scheitern kann folgender sein:

- Störung in der Kommunikation zwischen den Komponenten aufgrund der unterschiedlichen IGEL Netzwerktokens, siehe obigen Abschnitt "Nachrichten (see page 946)".

Weitere Prüfungen

Wenn andere Probleme festgestellt werden, werden hier die entsprechenden Ergebnisse und Lösungsvorschläge angezeigt.

Detaillierter Bericht

Ein detaillierter HTML-Bericht, der beim Klicken auf die Schaltfläche **Details anzeigen** generiert wird, bietet einige zusätzliche Informationen.

> **Tipp zur Kontaktaufnahme mit IGEL Support**
>
> Wenn die genannten Vorschläge zur Lösung der Probleme nicht geholfen haben, speichern Sie den HTML-Bericht und senden Sie ihn an den IGEL Support zusammen mit dem Archiv mit den Supportinformationen, das Sie in der Menüleiste unter **Hilfe > Supportinformationen speichern** erstellen können.

Rollen: Zeigt anhand der Ergebnisse an, welche Rollen für die Server der HA-Umgebung möglich sind.

Beispiel:

Process ID	Host	Roles
aa9ca121-2cd0-4f57-bee1-310f42045d84	HEX-02:	[WebdavServer, Server, HA, LoadBalancer, WebdavClient, Client]
ea75b934-2d26-45a3-b8eb-d9768489e560	HEX-01:	[WebdavServer, Server, HA, LoadBalancer, WebdavClient, Client]
ums-broker-50053-1594981900776-0-0	HEX-01:	[Server, HA, LoadBalancer, Client]
ums-broker-50125-1594982380105-0-0	HEX-02:	[Server, HA, LoadBalancer, Client]
ums-watchdog-50056-1594981903433-1-0	HEX-01:	[Server, HA, LoadBalancer]
ums-watchdog-50127-1594982383902-1-0	HEX-02:	[Server, HA, LoadBalancer]

Konfigurationsdaten: Zeigt die Konfigurationsinformationen an, wie sie von den Prozessen geliefert werden. Für einen UMS Load Balancer, d.h. einen UMS-Broker-Prozess, werden die bekannten Server dieses Load Balancers angezeigt.

Prozessinformationen: Liefert einen Überblick über die Prozesse.

Fingerprints der Zertifikate: Zeigt die Fingerabdrücke der Zertifikate an, die in der Datenbank auf dem UMS Server und in der tc.keystore-Datei auf dem UMS Load Balancer gespeichert sind.

IGEL UMS HA-Dienste und -Prozesse

Der folgende Artikel erläutert, welche Dienste und Prozesse bei der Installation der High Availability-Erweiterung (HA) der IGEL Universal Management Suite (UMS) ausgeführt werden. Es wird aber auch ein allgemeiner Überblick darüber gegeben, wie Sie Dienste und Prozesse für Ihre UMS Installation (nicht unbedingt für die UMS HA-Installation) neu starten können.

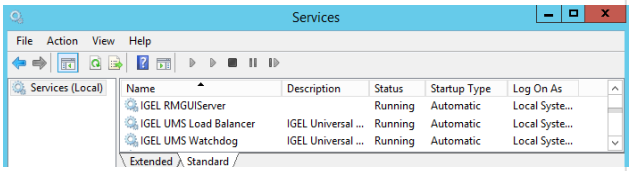
Eine HA-Installation (High Availability) besteht aus mehreren Prozessen: Auf jedem Knoten des HA-Netzwerks läuft entweder der UMS Server oder der UMS Load Balancer oder beide, abhängig von der Konfiguration, die Sie während des Installationsprozesses der UMS HA gewählt haben, siehe auch Konfigurationsoptionen (see page 911). Darüber hinaus läuft auf jedem Knoten immer der UMS Watchdog.

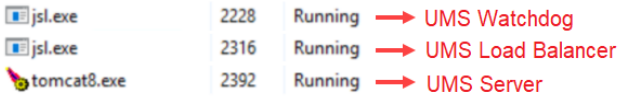
UMS Server	• Bearbeitet alle Anfragen von den Geräten und der UMS Konsole. • Spricht mit den Geräten. • Führt Aufgaben (Jobs) aus. • Agiert als Message Broker für interne Nachrichten.
UMS Load Balancer	• Leitet eingehende Anfragen von den Geräten an einen der UMS Server mit Lastverteilung weiter. Der UMS Load Balancer verfügt über eine Liste der laufenden UMS Server und verteilt die Anfragen an diese sequenziell.
UMS Watchdog	• Überwacht den Laufstatus des UMS Servers und des UMS Load Balancers, die auf demselben Server laufen, und leitet ihn an die UMS Server weiter. • Startet oder stoppt den UMS Server oder den UMS Load Balancer auf Anforderung eines UMS Servers.

⚠ Wenn sowohl der UMS Server als auch der UMS Load Balancer auf demselben Server laufen, verwendet der UMS Server Port 30002 und der UMS Load Balancer Port 30001. Wenn nur der UMS Server auf einem Server installiert ist, lauscht er immer auf Port 30001. Siehe IGEL UMS Kommunikationsports (see page 6).

Die folgende Tabelle zeigt, wie Sie herausfinden können, welche HA-Prozesse laufen und wie/wo Sie sie stoppen oder starten können.

Windows	Linux

Dienste:
 
 	
Normalerweise werden die Prozesse hier gestoppt.
	• Für die Liste der laufenden Prozesse verwenden Sie den Befehl:
	`sudo ps -ef | grep RemoteManager`
	wobei `RemoteManager` der letzte Teil des Installationspfades ist. Passen Sie diesen an, wenn der Installationspfad anders ist.
	Jeder Prozess hat zwei Einträge in der Liste.
	• Um die Prozesse zu stoppen, verwenden Sie:
	`sudo systemctl stop igel-ums-watchdog`
	`sudo systemctl stop igel-ums-broker`
	`sudo systemctl stop igel-ums-server`
	• Um die Prozesse zu stoppen, falls der Stopp mit den `init` -Skripten nicht funktioniert:
	`sudo kill -9 xxxx`
	wobei die ID des Prozesses folgenderweise herausgefunden werden kann:
	`sudo ps -ef | grep RemoteManager`

Task-Manager:  Notfallstopp, falls die Prozesse nicht in den **Diensten** gestoppt werden können.	

cmd / Command Prompt:
`sc queryex “IGELRMGUIServer”`
`sc queryex “IGEL UMS Load Balancer”`
`sc queryex “IGEL UMS Watchdog”`
Notfallstopp falls die Prozesse nicht in den **Diensten** gestoppt werden können:
`taskkill /PID xxxx /F`
wobei die PID folgenderweise herausgefunden werden kann:
`sc queryex “Name of the process”`	

Sie können den UMS Server-Dienst auch im **UMS Administrator > Distributed UMS** stoppen / starten, siehe Distributed UMS - Lokale UMS-Aktionen im IGEL UMS Administrator ausführen (see page 738).	

Shared Workplace (SWP)

IGEL Shared Workplace (SWP) erlaubt die nutzerabhängige Konfiguration anhand von Profilen, die in der IGEL Universal Management Suite angelegt und mit den AD-Benutzerkonten verknüpft werden. Dabei werden benutzerspezifische Profileinstellungen mit den geräteabhängigen Parametern gemeinsam an das Gerät übermittelt. Eine Übersicht der Parameter, die für einen Benutzer individuell konfigurierbar sind, finden Sie unter Im Benutzerprofil konfigurierbare Parameter (see page 959).

Lizenzierung für IGEL OS 11

Für den Einsatz mit IGEL OS 11-Geräten erfordert Shared Workplace eine gültige Lizenz aus dem Enterprise Management Pack (EMP). Diese Lizenz muss auf jedem IGEL OS 11-Gerät vorhanden sein, mit dem Shared Workplace verwendet werden soll. Wenn die Lizenz abläuft, kann sich kein Benutzer mehr bei einer Shared-Workplace-Sitzung anmelden.

Lizenzierung für IGEL OS 10

Für den Einsatz mit IGEL OS 10-Geräten erfordert Shared Workplace eine Add-on-Lizenz für Shared Workplace. Diese Lizenz muss auf jedem IGEL OS 10-Gerät vorhanden sein, mit dem Shared Workplace verwendet werden soll. Die Lizenz ist dauerhaft gültig.

Typische Beispiele für den Einsatz von Shared Workplace

- Schichtarbeitsplätze oder auch Callcenter, an denen verschiedene Anwender an einem Arbeitsplatz unterschiedliche Einstellungen benötigen, wie zum Beispiel Sitzungstypen oder Mauseinstellungen für Rechts- und Linkshänder.
- Roamingumgebungen, in denen die Anwender häufig den IT-Arbeitsplatz wechseln, wie zum Beispiel in Krankenhäusern, an Schaltern, Kassen oder Rezeptionen. Nach der Anmeldung des Nutzers konfiguriert sich das für Shared Workplace lizenzierte Endgerät automatisch über den UMS Server mit dem in der UMS Datenbank hinterlegten Einzel- bzw. Gruppenprofil. Die Zuordnung der Einstellungsprofile zum Benutzer erfolgt mithilfe der IGEL Universal Management-Konsole bequem und einfach per Drag & Drop.

> Mit zunehmender Anzahl an Shared Workplace-Arbeitsplätzen empfiehlt IGEL die Nutzung der UMS High-Availability-Erweiterung (see page 909). Die damit erzielte Hochverfügbarkeit des UMS Servers stellt sicher, dass Benutzer jederzeit ihr benutzerspezifisches Profil erhalten.

IGEL Tech Video

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=opgVxN791Vg

SWP-Konfiguration in der UMS Konsole

Um IGEL Shared Workplace nutzen zu können, müssen folgende Voraussetzungen erfüllt sein:

- Benutzer, die ein spezifisches Profil erhalten sollen, müssen in einem Microsoft Active Directory angelegt sein.
- Geräte, die eine Benutzeranmeldung erlauben sollen, müssen eine Lizenz für die Funktion IGEL Shared Workplace besitzen. Diese lässt sich über die Lizenzverwaltung der IGEL UMS an die Geräte übertragen.

  > Hat ein Gerät eine Lizenz für IGEL Shared Workplace erhalten, so kann dies nicht rückgängig gemacht werden. Die Funktion kann aber über die Liste der zur Verfügung stehenden Dienste in der Gerätekonfiguration abgeschaltet werden. Dann ist die Anmeldung über IGEL Shared Workplace deaktiviert.

- Nicht zwingend erforderlich – für größere Installationen jedoch empfohlen – ist der Einsatz der High-Availability-Erweiterung (see page 909) für die IGEL Universal Management Suite. Damit wird eine hohe Verfügbarkeit der Benutzerprofile im Netzwerk gewährleistet.

  > Sollten Sie IGEL Shared Workplace mit IGEL Universal Desktop WES 7 verwenden, so achten Sie darauf, dass für den Standardbenutzer **user** kein anderes als das Standardkennwort **user** gesetzt ist, eine Anmeldung ist sonst nicht möglich.

  Siehe auch Bildschirmkonfiguration für Shared Workplace (SWP) (see page 962).

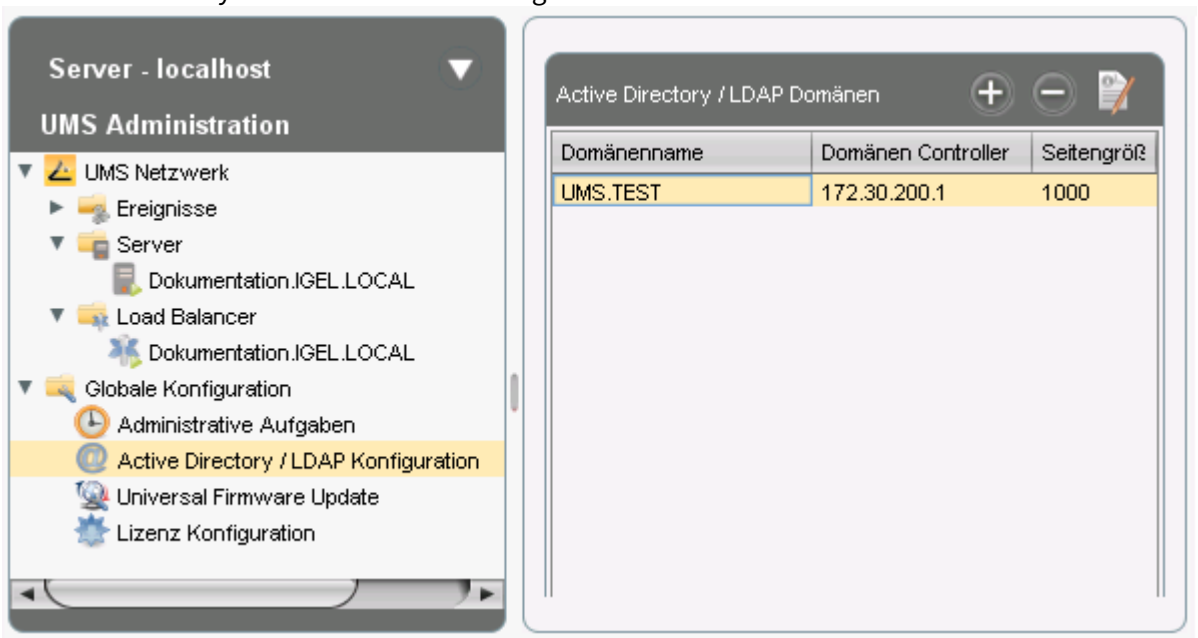
In diesem Kapitel erfahren Sie über:

Die Priorität benutzerspezifischer Profile wird in Wirkungsordnung der Profile in IGEL Shared Workplace (see page 402) behandelt. Siehe auch Wirkungsordnung von Profilen (see page 399).

Active Directory anbinden

So binden Sie in der UMS ein Active Directory ein:

1. Klicken Sie **Active Directory** im Bereich **UMS Administration**.
2. Klicken Sie **Hinzufügen**.
   Die Maske **Active Directory / LDAP-Service hinzufügen** öffnet sich.
3. Geben Sie **Domänenname** und die Zugangsdaten ein.
4. Bestätigen Sie mit **OK**.
   Ihr Active Directory wird nun in der Liste aufgeführt.



> Andere LDAP-Server (*Novell eDirectory*, *OpenLDAP* etc.) können nicht für die Benutzerauthentifizierung des *IGEL Shared Workplace* verwendet werden.

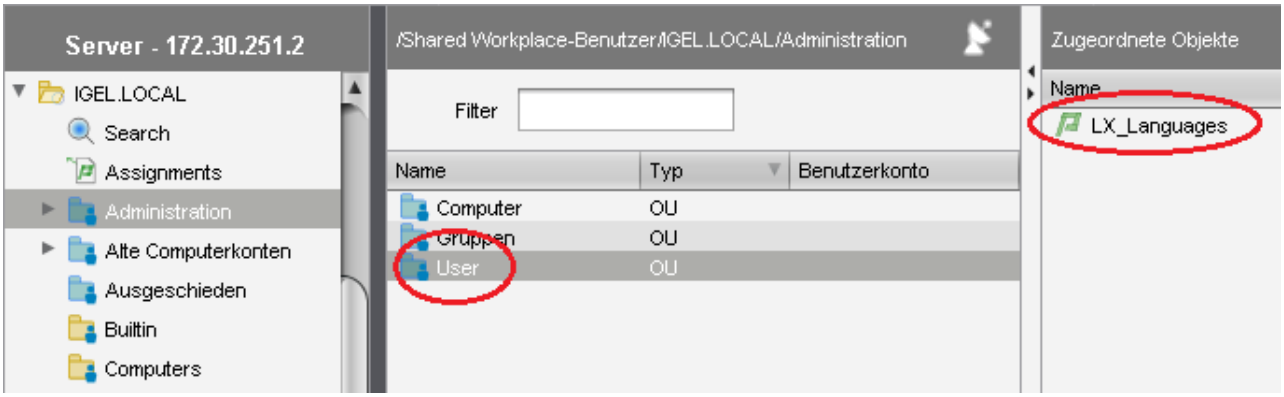
Benutzerprofil zuweisen

▶ Wechseln Sie in Ihr soeben eingerichtetes Active Directory im UMS Navigationsbaum unter **Server > Shared Workplace Benutzer**.

Sie können danach browsen oder über  danach suchen.

▶ Wählen Sie ein Objekt innerhalb der AD-Struktur aus.
Falls Sie bei der Konfiguration keine Benutzerdaten hinterlegt haben, müssen Sie sich gegenüber dem Active Directory authentifizieren.

▶ Klicken Sie **Server > Shared Workplace Benutzer > [Active Directory] > [Objekt]**, um diesem Objekt das gewünschte Benutzerprofil zuzuweisen:



Es können wie bei den Geräten auch mehrere Einzelprofile zugewiesen werden. Neben der direkten Zuweisung werden auch indirekt zugewiesene Profile berücksichtigt.

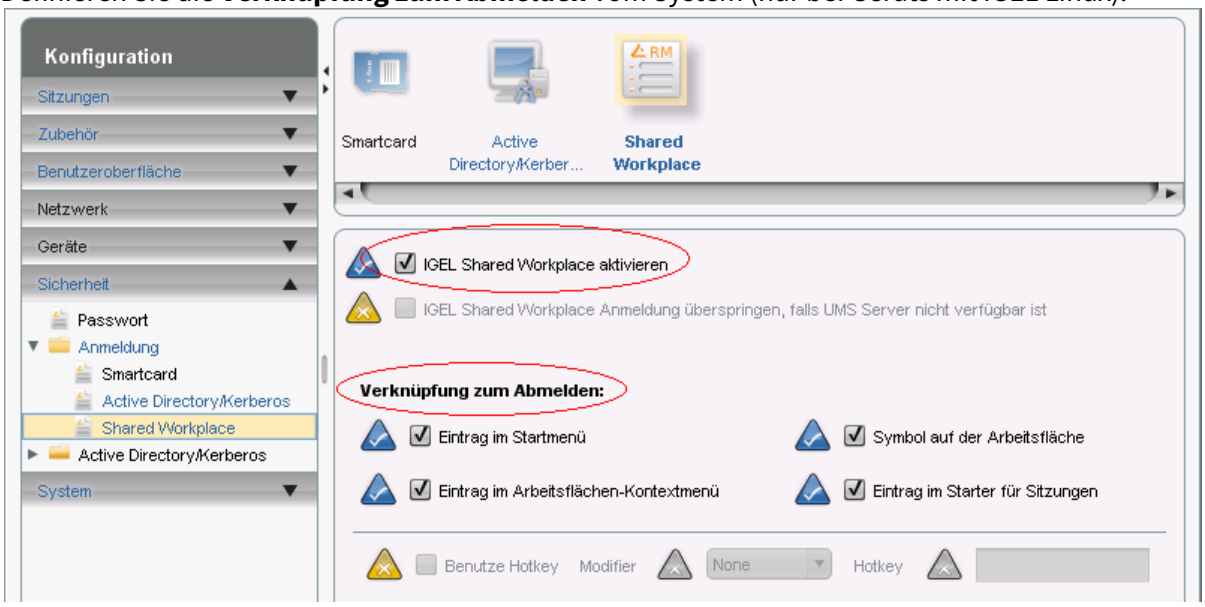
ⓘ Klicken Sie mit der rechten Maustaste auf den Namen eines Benutzerkontos, um die Profileinstellung auf einem speziellen Gerät zu sehen.

IGEL Shared Workplace am Gerät aktivieren

Die Einstellungen für Shared Workplace können sie von der UMS aus über ein Profil vornehmen, oder direkt im Setup des jeweiligen Geräts.

---

1. Gehen Sie auf **Konfiguration > Sicherheit > Anmeldung > IGEL Shared Workplace**.
2. Aktivieren Sie die Funktion **IGEL Shared Workplace**.
3. Definieren Sie die **Verknüpfung zum Abmelden** vom System (nur bei Geräts mit IGEL Linux).



Log-in des Benutzers

Sofern Sie eine Lizenz besitzen, können Sie sich einfach an einem Endgerät mit IGEL Shared Workplace anmelden:

1. Starten Sie das Gerät.
   Ein Anmeldefenster erscheint.
2. Melden Sie sich mit Ihren AD-Anmeldedaten an.
   Sie erhalten die Profileinstellungen, die in der UMS für Sie hinterlegt sind.

> Die aktive Konfiguration des Geräts für den angemeldeten Benutzer ergibt sich aus der Kumulation aller Profile, die dem Gerät oder dem Benutzer direkt oder indirekt zugewiesen wurden. Siehe dazu auch Priorisierung von Profilen in der IGEL UMS (see page 398).

Log-out und Benutzerwechsel

Windows Embedded Standard

- Melden Sie sich über das Startmenü ab.

IGEL Universal Desktop Linux

Unter Linux können Sie folgende Abmeldemöglichkeiten einrichten:

- Definieren Sie im **Starter für Sitzungen**, wo Sie die Schaltflächen zum Abmelden ablegen.
- Definieren Sie im IGEL Setup unter **Sicherheit > Anmeldung > IGEL Shared Workplace** einen Hotkey für die Abmeldung.

Im Benutzerprofil konfigurierbare Parameter

Nicht alle in der jeweiligen Firmware verfügbaren Parameter lassen sich benutzerspezifisch konfigurieren.

Im Folgenden sind die Systemeinstellungen beschrieben, die nicht wirksam durch ein benutzerspezifisches Profil konfigurierbar sind.

> In der UMS findet keine Prüfung statt, ob die Einstellungen wirksam sind.

Die **nicht wirksam** konfigurierbaren gerätespezifischen Systemeinstellungen der IGEL-Betriebssysteme sind im folgenden aufgelistet. Es findet keine Prüfung in der IGEL UMS statt.

- Universal Desktop Linux (see page 960)
- Universal Desktop Windows Embedded Standard (see page 961)

Gerätespezifische Parameter UD Linux

Im Benutzerprofil sind folgende Systemeinstellungen nicht konfigurierbar:

- Netzwerkeinstellungen inkl. der Netzlaufwerke
- Bildschirmkonfiguration bei IGEL Linux v5 bis *Version 5.05.100* und bei IGEL Linux v4 bis *Version 4.13.100*.

  > Unter *IGEL Linux Version 4.14.100* oder höher und *IGEL Linux Version 5.06.100* oder höher kann es abhängig von der verwendeten Hardware nach Änderung der Auflösung oder Rotation durch den Benutzer zu Darstellungsfehlern kommen. Hinweise zum Einrichten der Bildschirmkonfiguration für *IGEL Shared Workplace* gibt ein How-To (see page 962)-Dokument.

- Touchscreenkonfiguration
- Updateeinstellungen
- Sicherheitseinstellungen
- Remote Management
- Kundenspezifische Partition
- Server für Hintergrundbilder bei IGEL Linux *Version 10.03.100* oder niedriger

  > Ab IGEL Linux *Version 10.03.500* können Hintergrundbilder sowie Hintergrundbildserver benutzerindividuell über Shared Workplace definiert werden.

- Kundenspezifischer Bootbildschirm
- Browser-Plug-ins
- SCIM-Eingabemethoden, die Aktivierung ist aber benutzerspezifisch möglich
- Emulation 3-Tasten-Maus
- Appliance Mode (VMware View, Citrix XenDesktop und Spice)

Gerätespezifische Einstellungen UD W7

Diese Systemeinstellungen sind nicht im Benutzerprofil konfigurierbar:

- Sprache, Standards und Formate
- Netzwerkeinstellungen inkl. der Netzlaufwerke
- Active Directory-Anmeldung
- USB-Gerätekonfiguration
- Liste der verfügbaren Features und Windows Services
- Updateeinstellungen
- Setupsitzung
- Benutzer- und Sicherheitseinstellungen
- Dateibasierender Schreibfilter
- Energieoptionen
- Remote Management
- Appliance Mode (VMware View und Citrix XenDesktop)

Bildschirmkonfiguration für Shared Workplace (SWP)

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

As of IGEL Universal Desktop Linux *version 4.14.100* and *version 5.06.100*, Shared Workplace allows user-specific screen resolutions and configurations. Resolution, layout, refresh rate, rotation, number of screens, monitor connectors (DVI, VGA, ...) can be set per user, but color depth cannot.

There are technical limitations to user-specific settings: For VIA graphics drivers/hardware, the maximum desktop size is set in the `Screen` section of the X configuration file. The name and location of the X configuration file depend on the firmware version:

- IGEL Linux *version 10*: `/config/Xserver/xorg.conf-0`
- IGEL Linux *version 5*: `/config/Xserver/xorg.conf-0` or `/etc/X11/xorg.conf` (this is a symbolic link that points to `/config/Xserver/xorg.conf-0`)
  In the `Screen` section of the above-mentioned configuration file, you can find a line such as `Virtual 1920 1200`. The size defined here cannot be changed dynamically; it is a hard limit for the overall desktop size.

Best Practice

It is recommended to set the initial desktop configuration to the maximum number of screens and the resolutions to A `utodetect`. This way, the user-specific resolutions will not be restricted.

Debugging

If the total framebuffer size of the user-specific resolutions exceeds the limits of the `Virtual [width] [height]` setting from `/config/Xserver/xorg.conf-0` (or `/etc/X11/xorg.conf`), the user-specific resolutions cannot be activated and the screen configurations are not changed dynamically.

There is no warning dialog or anything else to alert the user to this restriction. But you can find related log messages via `journalctl` or in `/var/log/messages`:

```
XRANDR: ERROR: CANNOT APPLY CHANGES ->
```

```
XRANDR: ERROR: -> Selected modes ([width]x[height]) would exceed the maximum framebuffer size ([width]x[height])
```

Asset Inventory Tracker (AIT)

Weitere Informationen finden Sie unter Asset Inventory (see page 452).

IGEL Management Interface (IMI)

Hier geht es zur Dokumentation: IGEL Management Interface (IMI)

UMS Release Notes

UMS Release Notes stehen nur auf Englisch zur Verfügung.

Notes for Release IGEL UMS 12.04.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment IGEL UMS 12.04.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues IGEL UMS 12.04.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release IGEL UMS 12.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Troubleshooting: UMS Cannot Connect to the MS SQL Database

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment IGEL UMS 12.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features IGEL UMS 12.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues IGEL UMS 12.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 12.03.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 12.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment IGEL UMS 12.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features IGEL UMS 12.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues IGEL UMS 12.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Known Issues IGEL UMS 12.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 12.02.130

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 12.02.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release IGEL UMS 12.02.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release IGEL UMS 12.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment IGEL UMS 12.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Removed Support in IGEL UMS 12.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Added Support in IGEL UMS 12.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Known Issues IGEL UMS 12.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Limitations IGEL UMS 12.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features IGEL UMS 12.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues IGEL UMS 12.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release IGEL UMS 12.01.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment UMS 12.01.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features UMS 12.01.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues UMS 12.01.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Limitations UMS 12.01.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Known Issues UMS 12.01.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release IGEL UMS 6.10.150

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment IGEL UMS 6.10.150

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues UMS 6.10.150

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 6.10.140

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 6.10.140

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 6.10.140

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 6.10.140

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 6.10.130

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 6.10.130

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 6.10.130

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 6.10.130

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 6.10.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 6.10.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 6.10.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 6.10.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 6.10.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 6.10.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 6.10.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 6.10.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 6.10.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 6.10.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 6.10.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 6.09.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 6.09.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 6.09.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 6.09.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 6.09.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 6.08.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 6.08.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 6.08.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 6.08.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 6.08.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 6.08.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 6.08.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 6.08.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 6.08.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Known Issues 6.08.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 6.08.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 6.08.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 6.07.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 6.07.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Removed Support 6.07.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Added Support 6.07.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Known Issues 6.07.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 6.07.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 6.07.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 6.06.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 6.06.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 6.06.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 6.06.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 6.06.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 6.06.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 6.06.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Known Issues 6.06.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 6.05.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 6.05.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 6.05.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 6.05.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 6.05.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Removed Support 6.05.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Added Support 6.05.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Known Issues 6.05.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 6.05.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 6.05.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 6.04.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Software:	Version 6.04.120
Release Date:	2020-05-06
Release Notes:	RN-604120-1
Last update:	2020-05-06

Supported Environment 6.04.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

- **UMS Server:**

Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)

Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.5 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

Removed Support 6.04.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UMS Server

- Microsoft Windows Server 2008 (64 bit and with SP2) -> EOL 14.01.2020
- Microsoft Windows Server 2008 R2 (64 bit and with SP1) -> EOL 14.01.2020

UMS Client

- Microsoft Windows Server 2008 (64 bit and with SP2) -> EOL 14.01.2020
- Microsoft Windows Server 2008 R2 (64 bit and with SP1) -> EOL 14.01.2020
- Microsoft Windows 7 (64 bit and with SP1) -> EOL 14.01.2020

Backend database (DBMS)

- PostgreSQL 9.4 -> EOL Feb 2020

New Features 6.04.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

- Support of **OSCW** (IGEL OS Creator for Windows)

Resolved Issues 6.04.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Console, common

- Fixed: **Universal Firmware Update assignments** of devices were **not visible** in some cases.
- Fixed: In rare circumstances, the d**evice-specific command list** was **not complete**.

IGEL Cloud Gateway (ICG)

- Fixed: **Shadowing/SecureTeminal via ICG** always **used the internal ICG address and port** instead of the external address and port (if available).

Notes for Release 6.04.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Software:	Version 6.04.110
Release Date:	2020-03-12
Release Notes:	RN-604110-1
Last update:	2020-03-12

Supported Environment 6.04.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	with SP1
Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

Resolved Issues 6.04.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Jobs

- Fixed: **Jobs could not be edited/selected**. (Error Message was "`Error Unable to load details for the tree nodes. Original error message: null`")
- Fixed: A **missing library** could lead to **failing jobs on headless installations**.

Automatic License Deployment (ALD)

- Fixed: **Devices did not receive a renewal license** automatically if the renewed subscription pack was assigned to the UMS Licensing ID and the pack had no ALD Token.

Universal Firmware Update

- Fixed: The check for available firmware updates failed with a null pointer message if one of the downloaded firmware properties was invalid.

Searches

- Fixed: **Search History used lifetime settings of views** instead of its own lifetime settings.

Database schema

- Fixed: The **UMS could not be updated** if the used **schema name** contained **dashes**. (Only for Microsoft SQL Server databases)

Notes for Release 6.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Software:	Version 6.04.100
Release Date:	2020-02-17
Release Notes:	RN-604100-1
Last update:	2020-02-17

Supported Environment 6.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	with SP1
Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Microsoft SQL Server 2019	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

New Features 6.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UMS, common

- Added: **Shared Workspace** can be deactivated.
- Added: Support for **Secure Terminal via IGEL Cloud Gateway** (ICG 2.01.100 or higher and IGEL OS 11.02.100 or higher are required).
- Added: **Installer** and **UMS Administrator** perform **database version check** when a database is selected.
- Changed: It is possible to **log in to the UMS Server** via the UMS Console i**f the UMS Server is in HA update mode**.
- Added: '**Manual Licenses Dialog**' – Table with licensable devices shows the **list of licensing pack IDs** in the comment if the information is available in the UMS.
- Updated: Apache **Tomcat** from version 8.5.45 to **8.5.50**.
- Updated: **Java** from version 8u222 to **8u242**.

Universal Customization Builder (UCB)

- Added: **Universal Customization Builder** (for Windows) is now **available for free** (No license required).
- Removed: Obsolete **Linux part of Customization Builder**.

Jobs

- Added: **New Job** command '**Send Message**' added.

Universal Firmware Update

- Added: The UMS Server supports **FTP passive mode for Universal Firmware Upload**.
- Added: **Check for free disk space** on the file system **before downloading firmware updates**.

Console, administration section

- Added: Show **UMS Licensing ID fingerprint** in the **UMS Console** (**UMS Administration > Global Configuration > Licenses > UMS Licensing ID**).
- Changed: Option to enable **Master Profiles**, **Template Profiles** and **Recycle Bin moved to** new node **UMS Features** (**UMS Administration > Global Configuration > UMS Features**).
- Changed: It is now possible to choose **a specific port for the online check (UMS Administration > Server Network Settings > Online Check Parameters > Specify online check port (UDP)**).

Administrator application

- Added: Show **UMS Licensing ID fingerprint** in the **UMS Administrator** (Administrator application > **UMS Licensing ID Backup**).

- Added: **Multiselect** option **for cipher selection** (UMS Administrator > **Settings > Cipher > Configure Ciphers**).
- Added: **Confirmation dialog** after the database password change.

Notifications

- Added: Notifications for **expiring** and **expired certificates** (**Help > Notifications**).
- Added: Notifications for **expiring** and **expired packs** (**Help > Notifications**).
- Added: Option to **show archived notifications (Help > Notification**).
- Added: Option to **restore archived notifications**.
- Changed: Replaced the **"Do not show again" checkbox** for multiple notification selection with **a dropdown action selector** in the Notification dialog (**Help > Notifications**).
- Changed: **Notifications are automatically restored from the archive** when the Info Type is updated to a higher level (from warning to error).

Devices

- Added: **Device file location can now be edited** before sending a file to a device (Device context menu **> Other commands > 'File UMS > Device'**)

Views

- Added: If '**Send view result as mail**' ('View' context menu) fails, **an error message** is **displayed in the 'Messages'** area.
- Added: It is now **possible to send view results as mail** even **if the result is not loaded** in the detail view.

VNC

- Added: **Secure Terminal confirmation dialog** shows whether the terminal feature enabled status for each device.

IGEL Cloud Gateway (ICG)

- Added: The **Events table in the UMS Administration** view is always visible in the management tree. **ICG events will be logged in the table** (**UMS Administration > UMS Network > Events**)

Installer (Windows)

- Updated: **Bundled Microsoft Visual C++ 2017 Redistributable** from version 14.15 to **14.16**.

Resolved Issues 6.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UMS, common

- Changed: **Activation/Deactivation of template profiles/master profiles has to be confirmed now** when at least one key value/master profile exists.
- Fixed: Several **file choosers did not remember the last selected directory**.

Console, common

- Fixed: '**Messages**' area sometimes **forgot its previous size**.
- Fixed: Various **windows did not remember their last size**, **position** or had an unfavorable default size.
- Fixed: **Save support information** could sometimes not be generated due to the unnecessary size check.
- Added: **Cross-check of a user and group name** when adding a new administrator account.

Server, common

- Fixed: Removed misleading **logging information on updating network name for Linux** clients (`network.interfaces.ethernet.use_igel_setup`)

Devices

- Fixed: '**Runtime since last Boot**', '**Total Operating Time**', and '**Battery Level**' were **not always refreshed** on Refresh/F5.
- Fixed: **Changes to a device or a profile were lost** when switching to UMS Administrator in UMS Console.
- Fixed: **Update on network name (DNS) was not triggered** if name was changed via system information.

Firmware Customization

- Fixed: **Files** or **folders with spaces in the name** could not be used in **Firmware Customizations** or **file upload**.

Jobs

- Fixed: **Log messages for jobs** were not displayed.

Universal Firmware Update

- Changed: Snapshot upload in **'Universal Firmware Update' only allows** files with `.snp` **filename extension**.

Searches

- Fixed: **Changes to the Search result** page behavior (**Misc > Settings > Views and Searches > Page Behavior**) were **not applied immediately** after saving the settings and selecting a search result.

Configuration Dialog

- Fixed: "**Always apply settings on reboot...**" checkbox was **missing in Update time dialog** when saving Device/Profile configuration.

Console, administration section

- Fixed: The **split position of the panels** in the detail view of a server (**UMS Administration > UMS Network > Server**) was not persistent.
- Fixed: **Connect/Disconnect operation of ICGs to UMS HA** had inconsistent behavior.
- Changed: **Online Check Response Timeout input** restricted to **100 ms up to 10.000 ms** (**UMS Administration > Global Configuration > Server Network Settings**).

AD / LDAP integration

- Changed: For an administrator account import of users from an AD/LDAP directory (**System > Administrator account > Import**), the **selection for 'Add user/group' was improved**.
- Fixed: **Inherited permissions of an imported AD user** were **not displayed correctly** in the 'Effective Rights' section of the 'Administrator accounts' window (**System > Administrator accounts > Effective Rights**)

Console, web start

- Fixed: An issue introduced in UMS 6.03.120 prevented the **execution of the UMS Console via Java Web Start**.

VNC

- Fixed: **VNC Viewer always started on the primary screen** instead of the last screen (multidisplay environment).
- Fixed: The **VNC Certificate Dialog could be off-screen** and so blocked the user from interactions.

IGEL Cloud Gateway (ICG)

- Removed: Misleading **log message during ICG installation**.

Mobile Device Management (MDM)

- Fixed: **Synchronization with ICG** failed if the MDM push certificate had expired.

Administrator application

- Fixed: **Backup sizes smaller than 1 KB** were not displayed correctly.
- Added: **Additional check for the existing database schema** before activating a database connection.
- Added: **Check for supported database versions**.

High Availability Feature

- Fixed: **Misc settings** configurations (**UMS Administration > Global Configuration > Misc Settings**) were **not synchronized with all HA servers**.
- Fixed: **WebDAV subfolders** were **not synchronized with other HA servers**.
- Fixed: **Adding an HA server after adding an ICG server** to the environment **caused ICG connection problems**.
- Fixed: The created **support file**, from triggering 'Save support information' (**Help > Save support information**), **did not** always **contain** the **information of remote components**.

UI / Look&Feel

- Fixed: **Visibility** of various (disabled) **menu icons**.
- Removed: Deprecated **bevel bar from legacy themes**.

Notifications

- Fixed: **Notification dialog** did sometimes not show notifications **when global notifications were enabled**.

Notes for Release 6.03.130

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Software:	Version 6.03.130
Release Date:	2019-12-10
Release Notes:	RN-603130-1
Last update:	2019-12-10

Supported Environment 6.03.130

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	with SP1
Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

New Features 6.03.130

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UMS Common

- Changed: **All IGEL services** and resources like the **firmware update server** (which was fwu.igel.com[43] and is now fwus.igel.com[44]) and the **IGEL Knowledge Base** (kb.igel.com[45]) are now contacted via **HTTPS**. **It is now important to allow the https port (default 443) and the new address (**fwus.igel.com[46]**) in the firewall rules and the proxy rules**.

43 http://fwu.igel.com
44 http://fwus.igel.com
45 http://kb.igel.com
46 http://fwus.igel.com

Resolved Issues 6.03.130

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

IGEL Cloud Gateway (ICG)

- Fixed: **ICG root certificates** created with UMS version 6.01.130 or with an older version **can be used again for creating a signed certificate**.

Console, common

- Fixed: **The file transfer status** of firmware customizations without read permission was not displayed in the device detail window.

Firmwares

- Fixed: **Generic commands** could not be triggered by the UMS Console.

Notes for Release 6.03.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Software:	Version 6.03.110
Release Date:	2019-10-30
Release Notes:	RN-603110-1
Last update:	2019-10-30

Supported Environment 6.03.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	with SP1
Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

Resolved Issues 6.03.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UMS, common

- Fixed: Files are now applied correctly when assigned to multi-level device folders.

Console, common

- Fixed: Removed unnecessary log entries which occured if the user had no permission set.
- Fixed: Issue where the 'configuration changed' indicator (blue exclamation mark) was not updated correctly if shared workplace assignments existed.

Views

- Fixed: Amount of hidden devices did not get refreshed if devices were added by another console.

Notes for Release 6.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Software:	Version 6.03.100
Release Date:	2019-10-15
Release Notes:	RN-603100-1
Last update:	2019-10-15

Supported Environment 6.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	with SP1
Microsoft Windows 8.1	(64 bit)	with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	with SP2
Microsoft Windows Server 2008 R2	(64 bit)	with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

Red Hat Enterprise Linux (RHEL) 8	(64 bit)	

- **Backend Database (DBMS):**

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
Oracle 11g R2	
Oracle 12c	
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10.9 - 10.14

Known Issues 6.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

- **Updating IGEL Windows 10 devices via UMS webdav folder** can result in **an endless update loop** of the devices. Please contact IGEL Support in this case.
  To avoid this problem, we recommend distributing the Windows 10 firmware updates via an external FTP or HTTPS server.

New Features 6.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UMS, common

- Added: New display of **legend of UMS icons** (UMS Console **> Help > Legend**).
- Added: Support of **MS SQL Server Always On Availability Groups**.
- Added: Allow **TLS protocol** version **1.1 or 1.2 selection for SMTP server** communication in UMS.
- Changed: UMS with **external Derby database** supports only **Derby** versions **10.9 up to 10.14**.
- Changed: Increased the **maximum memory usage** of **UMS Console** (1024mb -> 3072mb), **UMS Server** (2048mb -> 4096mb) and **RMAdmin** (512mb -> 1024mb).
- Changed: Redesign of the UMS cache. The **cache is now always switched on**. The corresponding configuration dialogs were removed.
- Updated: **Apache Tomcat** from version 8.5.43 to **8.5.45**.
- Updated: **Azul Zulu JRE** from version 1.8.0_212 to **1.8.0_222**.

Console, common

- Added: **Configuration dialog for Views** and **Searches** (**Misc > Settings > Views and Searches**).
- Added: **Digit grouping** to improve the readability of large numbers (e.g. devices in a folder).
- Added: When creating a new administrator account, the **user name** or **group name** is **checked for duplicate names** prior to saving (**System > Administrator accounts > New**).

Devices

- Added: Option to **copy device information** to clipboard **in ASCII format** (**Device** > Detail View > Bottom > **Copy to Clipboard (ASCII)**).
- Changed: **Import Devices** uses the **Unit ID** instead of the MAC address as the client descriptor **for the long and short import formats**.
- Changed: **States of Device information lists** ("open" or "close") are now saved.

Views

- Added: **Option to cache View results** for more convenience.

Universal Firmware Update

- Changed: **Windows Firmware Updates** are now provided **with https**.
- Added: **Universal Firmware Update** supports **FTPS** and **SFTP** (**UMS Administration > Global Configuration > Universal Firmware Update**).

Searches

- Added: **New View/Search criterion** 'Structure Tag'.
- Added: Option to **save Searches** as **CSV, XML, HTML**, and **XSL**.
- Added: **Option to cache Search result**s for more convenience.

Console, administration section

- Added: **Choice** between **rich** and **plain text messages** to a device (**UMS Administration > Global Configuration > Messages to Devices**).
- Changed: Available **filter criteria** for registered device licenses (**UMS Administration > Global Configuration > Licenses > Device's Licenses**).
- Changed: It is now possible to **create/import certificates** in the **remote ICG installer/updater**. (UMS Console > **UMS Administration > UMS Network > IGEL Cloud Gateway**).

High Availability Feature

- Added: **'Stop Service' option** in process detail view (**UMS Administration > UMS Network > Server/Load Balancer**).

Installer (Linux)

- Added: **UMS** can be installed **on Red Hat Enterprise Linux 8**.
- Added: Installer will now also **check for a running instance of UMS Administrator** during an update installation.
- Added: **New wizard page** after component selection, **displaying the memory (RAM) requirements** for the selected components.

Installer (Windows)

- Added: **New wizard page** after component selection, **displaying the memory (RAM) requirements** for the selected components.

Resolved Issues 6.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UMS, common

- Fixed: **Deleting a firmware update snapshot** also **deleted the** `ums_filetransfer` **folder**. (Only occurred if the firmware update has been stored directly in the UMS webdav folder without parent folder).

Console, common

- Fixed: **Indicator that the device settings have change**d (blue exclamation mark) **did not always appear** when an assigned profile was changed or indirectly assigned to a device.
- Fixed: When using an Oracle database, after moving files/views to a subfolder **the file/view count display of the subfolder was not updated**.
- Fixed: The **"Show Message" button** (UMS Console > Bottom right hand corner) **in "smart contrast"** behaves now analogously to the other themes.
- Fixed: The **UMS firmware statistics** overview (**Misc > Firmware Statistics**) could display **a wrong number of devices** when UD Pocket devices were managed in the UMS.
- Fixed: When a firmware customization has been assigned to a device, this device and all other already assigned devices got a **notification that the settings have changed**. Now only the new device will get the notification.
- Fixed: **Overwriting an existing zip file** when exporting firmware, firmware customizations, template keys / groups and device settings **created an unusable file** (**System > Export...**).

Devices

- Changed: The value o**f 'Last IP' in 'System Information'** of a device **is no longer editable** and has been moved from the editable section to the non-editable section.
- Fixed: Possible problems with the **File Transfer Status** if the device is **connected via ICG**.
- Changed: **Renamed** the field 'Expiration Date of Maintenance Subscription' **to** '**Expiration Date of OS10-Maintenance Subscription'** in the device detail view to avoid confusion (**Device** > Detail View > **Advanced System Information**).

Profiles

- Fixed: '**New Profile' dialog did not resize** if expert mode was closed (UMS Console > **Profiles** > context menu > **New Profile**).

Views

- Fixed: **Creating a view with criterion 'Monitor size'** caused an **error with the SQL Server database**.

Configuration Dialog

- Fixed: In the configuration dialog of a device on the **Security > Password** page, the "**Change Password" buttons** are now **properly enabled/disabled** to match the enable states of the corresponding parameters.
- Fixed: In profile configuration dialog (**Devices > Storage Hotplug**), the "Storage Hotplug" selection was not saved.

Console, administration section

- Fixed: Display of **wrong status** after renaming a server (**UMS Administration > UMS Network > Server**).
- Added: **Syntactic check of email address** before sending email in Cloud Gateway Options (**UMS Administration > Global Configuration > Cloud gateway options > First authentications keys > Send first Email authentications keys by Email**).

Firmware Customization

- Fixed: **Importing a firmware customization** without assigned files resulted in a "permission denied" warning.

Mobile Device Management (MDM)

- Fixed: **MDM** is working again **with LDAP users**.

Server, common

- Changed: Server details (**UMS Administration > Server**) will now show the **actual name of the Linux operating system** if it provides the file `/etc/os-release`.

High Availability Feature

- Fixed: **Support information for HA feature** no longer generates error-entry on other servers.
- Fixed: Issue with data directory in HA update. **HA update changed the data directory** (`ums_filetransfer`) to `c:\programData\igel` **without notice**. All files were automatically moved to the new directory. On Linux systems, the issue could lead to loss of files in `ums_filetransfer` folder.

UI / Look&Feel

- Fixed: **Console used wrong tooltip color** after sending RichMessages.

Installer (Linux)

- Fixed: After an **upgrade installation of the UMS Load Balancer**, it did not talk to the UMS Server anymore.

Notes for Release 6.02.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Software:	Version 6.02.110
Release Date:	2019-08-14
Release Notes:	RN-602110-1
Last update:	2019-08-14

Supported Environment 6.02.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	New: only with SP1
Microsoft Windows 8.1	(64 bit)	New: only with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **Backend Database (DBMS):**

Oracle 11g R2	
Oracle 12c	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10

New Features 6.02.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Server, common

- Updated **Apache Tomcat** from version 8.5.40 to **8.5.43**

IGEL Cloud Gateway (ICG)

- Added: Support for **Shadowing via IGEL Cloud Gateway** (ICG 2.01.100 or higher and IGEL OS 11.02.100 or higher are required)

Resolved Issues 6.02.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

AD / LDAP integration

- Fixed: **AD authentication** was not possible in a mixed domain/subdomain environment.

Thin clients

- Fixed: **Firmware update settings** of a device shown in UMS differed from the settings the device received when a **Universal Firmware Update** and a **profile with configured firmware update settings** were assigned to the device.

Views

- Added: The **timeout for the online check of devices** that is set in **UMS Administration > Global Configuration >Server Network Settings > Online Check Parameters** will be used for the **Online criterion** in **Views**.

IGEL Cloud Gateway (ICG)

- Changed: Due to structural changes between ICG 1.04 and ICG 2.01 **a downgrade is not possible**. It is also disabled in the ICG remote installer.
- Fixed: **Changing the name** of an ICG or a UMS Server does no longer result in an error message.

DB command line tools

- Fixed: The **embackup command line tool didn't find the backup file in restore mode** although it existed.

Server, common

- Fixed: Downloading global notifications (by UMS itself or via the **Send notification information via mail** administrative task) failed with Microsoft databases.

Installer (windows)

- Fixed: **Updating a UMS installation (4.09.x or older) directly to versions between 5.09.100 and 6.02.100 (inclusive) did not work completely**. In these cases, the installer asked for the data directory (which already existed) and even if the user entered the same path as the UMS used before, the folder was completely overwritten. Additionally, if the UMS used an embedded database before the update, a manual reactivation was sometimes required after the update.

Notes for Release 6.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Software:	Version 6.02.100
Release Date:	2019-06-14
Release Notes:	RN-602100-1
Last update:	2019-06-14

Supported Environment 6.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	New: only with SP1
Microsoft Windows 8.1	(64 bit)	New: only with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **Backend Database (DBMS):**

Oracle 11g R2	
Oracle 12c	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10

New Features 6.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UMS (common)

- Added: **Disk Usage** notification type for the UMS notification system. (**Help > Notifications**)
- Added: **Global notification** type for the UMS notification system to inform the user of important news like maintenance times, bugfixes, etc. (**Help > Notifications**)
- Changed: When a device is renamed, the setting **Adjust network name if UMS-internal name has been changed** is automatically set to enabled (**UMS Administration > Global Configuration > Device Network Settings > Adjust Names of Devices**).
- Changed: The administrative task **Assign objects to the devices of views** now provides the possibility to **assign firmware customizations**, **files** and **firmware updates** to the devices of views.

Console (common)

- Added: **Administrative tasks** notification type for the UMS notification system. (**Help > Notifications**)
- Added: The UMS now **displays all connected monitors** of a device. It previously displayed only two.

Console (administration section)

- Added: Option to create **ICG wildcard certificates**. (**UMS Administration > Cloud Gateway Options > Create signed certificate**)

Server (common)

- Changed: Suppress **server identity** in tomcat headers and by disabling default error pages.

AD / LDAP integration

- Added: **LDAPS** support **for AD** configuration.

Mobile Device Management (MDM)

- Added: **Public port** and **address** are now part of the MDM enrollment codes.

Security Fixes 6.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

High Availability Feature

- Fixed: HA installation unnecessarily **opened a debug port** (**ISN 2019-05**).

Resolved Issues 6.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UMS (common)

- Fixed: **Resetting** a device **to factory defaults** could lead to various errors. (**UMS > Device > [Device's context menu] > Other commands > Reset to Factory Defaults**)
- Fixed: Missing **configuration state change flag** for template value and value group assignments.
- Fixed: Text **color of warning hints** when some/none of the selected devices have **Secure Terminal** enabled.
- Removed: Unused icons.
- Changed: **Tomcat access log files** are now also collected as a part of the support information. (**UMS > Help > Save support information**)
- Changed: The bundled Oracle JRE was replaced with **Azul Zulu JRE 8 Update 212**.
- Updated: **Apache Tomcat** from version 8.5.37 to **8.5.40**.
- Updated: UMS-bundled Java version from **Java 8** Update 202 to **Update 212**.

Console (common)

- Fixed: Already existing **archive of a profiles export** could not be overridden.
- Fixed: **UMS console login dialog** was not properly focused.
- Fixed: **Notifications** cannot be deactivated for **users of an imported AD group**.
- Fixed: Some texts could not be read because the text and the background had the same color.
- Added: Functionality to **assign objects** (profiles, FWCs, etc.) to more than one device at once.
- Fixed: Error message when **exporting result in SQL** console. (**Misc > SQL Console > Save Result**)
- Changed: In the UMS **Scan for devices** dialog, when the **Rescan** action is executed, the current filter is maintained and applied again to the new scan results. (**UMS > Scan for devices > Scan > Rescan**)
- Fixed: Double click on **Indirect assigned objects** redirects you to the Object and on right-click a pop-up window opens.
- Fixed: Selecting '**Don't show again**' on a notification in the **Notification** dialog had no effect. (**Help > Notifications**)
- Fixed: Wrong color in **Move to recycle bin** confirmation dialog.
- Fixed: Issue when devices were erroneously shown as unlicensed.
- Fixed: Issue when the **Close** button was sometimes invisible in the **Update Check** dialog. (**Help > UMS Update Check**)
- Changed: **Notification pop-up** on start-up is hidden if there are no notifications.

Devices

- Changed: **Save device files for support** dialog was redesigned and completed with the possibility to save files of multiple devices and devices of views. (**Help > Save device files for support**)
- Changed: **Wake up** commands are not sent to devices when they are registered in the UMS through an ICG.

Profiles

- Fixed: Re-added a missing **file picker** for the field **File name** on page **System > Update > Snapshots > Download**. File picker is now properly enabled after resetting the file name parameter with enabled template keys checkbox.
- Fixed: Changes of the **screen rotation**, i.e. rotating a screen with the left/right arrow buttons on the **User Interface > Display** page, could not be saved in profiles.
- Fixed: Re-added a missing **FTP password** field in W7 profile configuration dialog. (**System > Snapshots > Upload/Download**)
- Changed: Simplified dialog to create a new profile.

Template Keys and Groups

- Fixed: **Variable expressions** in template keys are now supported for **devices registered into directories**.

Firmware Customization

- Fixed: The **FWC import** did not upload the provided files.
- Changed: The **Firmware Customization import file** is validated and the import process is aborted if the imported parameters are not supported by the current UMS version.

Views

- Fixed: **CSV-exports** did not include the **column headers** of custom device attributes. (Admin task: Export view as...)
- Fixed: **Special characters from Eastern Europe** are shown incorrectly within **view exports**. (**View context menu > Save as...**)
- Fixed: Reduced processing time of assignment/detachment of profiles to/from the devices of a view.
- Added: A new **View** criterion for **device licenses**.

Jobs

- Changed: By **deleting a server** in **UMS Administration > UMS Network > Server**, the assigned devices are assigned to another available server and the **Job** execution data is deleted.

Automatic License Deployment (ALD)

- Fixed: An **empty error message** is shown if the configuration of **UDC2 Deployment** is changed and the configuration page is left without saving the changes.
- Fixed: A **Product Pack** is occasionally shown twice in the **Registered packs** section. (**UMS Administration > Global Configuration > Licenses > Deployment**)
- Changed: The **default automatic distribution method of new packs** (except for Workspace Edition packs) altered from 'Enabled' to 'Enabled (with conditions)'.

Universal Firmware Update

- Fixed: A **device directory** cannot be assigned to a **Universal Firmware Update** if the directory has already such an assignment.
- Changed: The **progress bar** shows the **download process** of Universal Firmware Update with **a better accuracy**.

Configuration Dialog

- Fixed: Configuration dialog combobox **Multimonitor full-screen mode** was missing in UMS 6 for **clients with firmware 10.4.100**. (**Sessions > Citrix XenDesktop/XenApp > HDX/ICA Global > Window**)

Console (administration section)

- Changed: A test mail configured under **UMS Administration > Mail Settings > Send Test Mail** can now be sent to different recipients.
- Fixed: The **Certificate Management Node** was only visible to the **DB administrator**. (**UMS Administration > Global Configuration > Certificate Management**)
- Fixed: Issue when multiple **ICGs** were shown in the wrong order. (**UMS Administration > UMS Network > Igel Cloud Gateway**)
- Updated: **DSA** export graphic. (**UMS Administration > Global Configuration > Licenses > Device's Licenses > Export Unit ID list**)
- Fixed: In the device's **Rich Message Editor**, the **Reject changes** message does not appear anymore if you switch the template and the previous template had no changes. (**UMS > Device > [Device's context menu] > Other commands > Send Message**)
- Fixed: **UMS Licenses** with more than one corresponding notification could not be deleted. (**UMS Administration > Global Configuration > Licenses > UMS Licenses**)
- Added: **Wait dialog during ICG certificate creation** to indicate progress. (**Global Configuration > Cloud Gateway Options**)
- Added: **Server** and **broker icons** now show status.
- Changed: Renamed '**Remove'** buttons in the **ICG configuration dialog** to avoid misunderstanding. (**UMS Administration > UMS Network > Igel Cloud Gateway**)
- Added: **Dialog to Naming Convention** feature to guide the user. (**Global Configuration > Device Network Settings > Naming Convention**)
- Fixed **display** of correct **operating system name** for Windows Server 2016/2019 in administration section.

Console (web start)

- Fixed: Webstart sometimes showed **outdated splash screen**.
- Added: **Expressive error and log messages** when uploading files to UMS server fail due to **invalid server hostname**.

WebDAV

- Fixed: **WebDAV credentials** were not recognized under certain circumstances.

IGEL Cloud Gateway (ICG)

- Fixed: **UMS lost ICG connection** if a lot of devices were ICG administrated (device count> 500).
- Changed: When a device is registered on ICG, **ICG credentials** are **cached** before the device is removed from the **Recycle Bin** and then stored again. It only applies for devices that are in the Recycle Bin at the moment of ICG registration.
- Added: **New safeguard** to the ICG certificate dialog to prevent inexperienced users from making mistakes. (**UMS Administration > Global Configuration > Cloud Gateway Options**)
- Added: Option for the **certificate creation dialog** whether a new certificate should be **CA** or **End Entity**.
- Added: Check to prevent users from signing a certificate with a non-CA certificate.
- Added: **X.509 extensions** to show certificate dialog.

Server (common)

- Updated: **Microsoft SQL Driver** to support **TLS 1.2** in Microsoft SQL database connection.
- Fixed: Issue with an **incorrect identification** of the operating system of **Windows Server 2016/2019**. (**UMS Administration > UMS Network > Server > [UMS Server] > Attribute 'Operating System'**)
- Fixed: A **valid Workspace Edition license / Enterprise Management license** was not recognized because of not properly formatted timestamps.
- Fixed: Bug in the device authentication.
- Changed: All tables of the database schema are optimized. (Optimize Database)
- Updated: **EULA** text.

High Availability Feature

- Fixed: HA installation unnecessarily **opened a debug port**. (**ISN 2019-05**)
- Fixed: Communication issues within a HA network.
- Fixed: **Update installation wizard** contained misleading user prompt.
- Fixed: Commands for servers, load balancers and ICGs could create an **unreadable balloon tip**.
- Changed: Now support files also contain **watchdog log files** in **Save support information** function. (**UMS > Help > Save Support Information**)

Installer (Linux)

- Fixed: **Uninstaller on Linux** can be executed from now on only with **root privileges** and shows the correct UMS version.
- Fixed: **Splash screen** was shown as "**win0**" on panel in GNOME desktop on **RHEL7** and **Oracle Linux 7**.
- Added **check for running UMS** Console in Linux installer.
- Fixed: **UMS binaries** (e.g. RemoteManager.bin) do not start on **RHEL 7.x** or **Oracle Linux 7** due to ABI compatibility issue.

UI / Look&Feel

- Fixed: **Rich Message Templates** could spill their colors into the UMS.

Notes for Release 6.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Software:	Version 6.01.100
Release Date:	2019-02-15
Release Notes:	RN-601100-1
Last update:	2019-02-15

Supported Environment 6.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **UMS Client:**

Microsoft Windows 7	(64 bit)	New: only with SP1
Microsoft Windows 8.1	(64 bit)	New: only with Update 2919355
Microsoft Windows 10	(64 bit)	
Microsoft Windows Server 2008	(64 bit)	New: only with SP2
Microsoft Windows Server 2008 R2	(64 bit)	New: only with SP1
Microsoft Windows Server 2012	(64 bit)	
Microsoft Windows Server 2012 R2	(64 bit)	New: only with Update 2919355
Microsoft Windows Server 2016	(64 bit)	
Microsoft Windows Server 2019	(64 bit)	
Ubuntu 16.04	(64 bit)	
Ubuntu 18.04	(64 bit)	
Oracle Linux 7	(64 bit)	
Red Hat Enterprise Linux (RHEL) 7	(64 bit)	

- **Backend database (DBMS):**

Oracle 11g R2	
Oracle 12c	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10

New Features 6.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Automatic License Deployment (ALD)

- Added: Support of new **IGEL OS 11 licensing mechanism** and new license distribution method **Automatic with Condition**. With this option, the device will get a license automatically only when the device accords to one or more of the selected conditions. The conditions can be folder memberships or views.
- Added: New **UMS Licensing ID** for easier license deployment. (**UMS Administrator > UMS Licensing ID** and **UMS Console > UMS Administration > Global configuration > Licenses > UMS Licensing ID**)

UMS (common)

- Updated: **Apache Tomcat** from **version 8.5.32 to 8.5.37**.
- Updated: UMS-bundled Java version **from Java 8 Update 181 to Update 202**.
- Added: Support for **Windows Server 2019**.
- Added: It is now possible to **license devices via context menu** (**License manually ...** in context menu of **Devices**, **Device Directories** and **Views**).
- Added: **Device-specific commands** that can be executed in the device's context menu (**UMS > Structure Tree > Devices**) and in the **device's menu bar**. The list of the available commands depends on the current selection. Therefore, a command is only listed when it is possible to execute by at least one of the devices in the current selection. The specific commands can be also selected in **Jobs**. (**UMS Console > Management Tree > Jobs**)

Resolved Issues 6.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UI / Look&Feel

- Changed: **New bootsplash and theme** for UMS 6.01.100

IGEL Cloud Gateway (ICG)

- Changed: **Stabilized ICG connections** in UMS High-Availability Environments (UMS HA)
- Fixed: **Sub-Certificates (ICG) were not visible** right after creation. A refresh was necessary.
- Fixed: A **used mass deployment key** was not exportable. (**UMS Console > Global Configuration > Cloud Gateway Options**)
- Fixed: The **usage count of first-authentication keys** did not change. (Affected: Only the GUI representation in **UMS Console > Global Configuration > Cloud Gateway Options**)

UMS (common)

- Fixed: All **certificate management actions**, which generate a new network token, failed to save the network token. (Only in HA environment)
- Changed: **Thin Clients** have been renamed "**Devices".**

Console (common)

- Fixed: The download link in **UMS Update Check** could not be opened on some operating systems. (**UMS Console > Help > UMS Update Check**)

Devices

- Fixed: The function **Take over settings from...** did not work, when the UMS was connected to a PostgreSQL database. (**UMS Console > device > context menu**)
- Fixed: Sometimes an **empty error dialog** occurred by selecting a device (happened only if an assigned file has been deleted before).

Firmware Customization

- Fixed: The **manual import of firmware customizations** from older UMS versions was not possible. (**UMS Console > System > Import > Import Firmware Customizations**)

Automatic License Deployment (ALD)

- Fixed: **Changing the default proxy in the GUI did not change the default proxy in the backend** sometimes. (Only a server restart fixed the bug)
- Changed: Improved the **token validation dialog** to be more user friendly. (**UMS Console > Global Configuration > Licenses > Deployment > Register Pack**)

Console (administration section)

- Changed: Improved **certificate validation mechanism** (**UMS Console > Global Configuration > Certificate Management**)
- Fixed: The **'host' entry in ICG remote installer dialog** is now editable for **wildcard certificates** (e.g.: *.xyz.com[47]). (**UMS Console > Administration Tree > UMS Network > Igel Cloud Gateway > Install new ICG Cloud Gateway**)

Administrative tasks

- Fixed: The administrative task **Create backup** failed for external databases when the task was configured to **include licenses and files**, which is only possible for the **embedded database**. (**UMS Console > Administration Tree > Global Configuration > Administrative Tasks**)
- Fixed: An issue where the **next execution time of admin tasks** was not properly calculated. (**UMS Console > Administration Tree > Global Configuration > Administrative Tasks**)

Server (common)

- Fixed: The **certificate key pair import fails**, if the UMS data directory differs from the default. (**UMS Console > Administration Tree > Global Configuration > Certificate Management**)

Administrator application

- Fixed: It was not possible to **delete created database backups** even after a restart of the UMS Administrator.

Installer (Linux)

- Fixed: The **update installation** on Linux OS will no longer ask for the **installation directory**.

47 http://xyz.com

Notes for Release 5.09.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Software:	Version	5.09.100
Release Date:	2018-10-08	
Release Notes:	Version	RN-509100-1
Last update:	2018-10-08	

The following formatting is used in the document:

format type	example	use
bold and underlined	enable/disable	the default setting of a value
bold and arrow	**menu > path**	menu path in the IGEL setup
bold	**GUI** [keyboard]	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	**[session name]**	variable values

Supported Environment 5.09.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 16.04	(64 bit)
Ubuntu 18.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **UMS Client:**

Microsoft Windows 7	(64 bit)
Microsoft Windows 8	(64 bit)
Microsoft Windows 10	(64 bit)
Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 16.04	(64 bit)
Ubuntu 18.04	(64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **Backend database (DBMS):**

Oracle 11g R2	
Oracle 12c	

Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL	9.4 - 9.6 and 10.1
Apache Derby	10

Warnings 5.09.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

- Following 32-bit environment is no longer supported:
  (Support removed because of software change to 64 bit)

  UMS Server:

  Ubuntu 14.04 (32 bit)
  Ubuntu 16.04 (32 bit)
  Red Hat Enterprise Linux (RHEL) 6 (32 bit)

  UMS Client:

  Microsoft Windows 7 (32 bit)
  Microsoft Windows 8 (32 bit)
  Microsoft Windows 10 (32 bit)
  Ubuntu 14.04 (32 bit)
  Ubuntu 16.04 (32 bit)
  Red Hat Enterprise Linux (RHEL) 6 (32 bit)

- Microsoft SQL Server 2008 / 2008 R2 support removed because of incompatible SSL certificates (not supported by Java)
- Ubuntu 14.04 (64 bit) support removed because of incompatible libraries (too old for the new UMS installation files)
- Increased maximal memory usage:

  UMS Server: 1024 MB to 2048 MB
  UMS Client: 768 MB to 1024 MB
  UMS Administrator: 384 MB to 512 MB

- Removed function to create a thin client license with smartcard. (**UMS Administration -> Global Configuration -> Licenses -> Thin Client Licenses -> Hardware**)

Care:

Licenses can still be created via Thin Client Smartcard License Server. (**UMS Administration -> Global Configuration -> Licenses -> UDC2 Deployment**)

New Features 5.09.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UMS Common

- **New EULA**: This UMS version is licensed under a new end user license agreement (EULA). Please read it carefully.
- Added: **Notifications**. Now the UMS Console shows a notification pop-up (default: on each console connect) which informs about the latest firmware updates and expiration of UMS or client licences. Notifications can be deactivated (for all users) in **UMS Console -> Administration Tree -> Global Configuration -> Misc**, and the relevant notification types can be set in **UMS Console -> Misc -> Settings -> Notifications** (user specific). Notifications can also be sent via Mail. (**UMS Console -> Administration Tree -> Global Configuration -> Administrative Tasks**)
- Added: It is now possible to **configure the used cipher suites for the UMS SSL port**. This setting is server specific and not part of the database backup. For UMS HA: Cipher suite selection has to be made on each node separately. (**UMS Administrator -> Settings -> Configure Ciphers**)
- Added: New feature **Certificate Management**: It is now possible to replace the certificate, which is mainly used for thin client to UMS communication. Changing the default certificate triggers a mechanism which consistently tries to store the new certificate on each thin client. This can only be done for online thin clients.

  Warning

  Incautious usage can lead to loss of the management connection to thin clients. The management functionality can only be restored by deleting the UMS certificate manually (local access) from each affected thin client. Certificate management can be found in **UMS Console -> UMS Administration -> Global Configuration -> Certificate Management**. (Only visible for the database administration user)
- Updated: The UMS is now bundled with a 64 bit JRE. The new JAVA version is 1.8.0_181.

Thin Clients

- Added: **Automatic Wake On LAN Proxy Detection**. The UMS will try to find a thin client that is able to relay the wake up call automatically to the target thin client without configuring thin clients as Wake On Lan Proxy. A thin client can automatically relay the wake up call, if the thin client is online, has a firmware version of LX 5.09.100 or newer and can 'see' the target thin client (same network, subnet ...). This feature can be activated in **UMS Console -> UMS Administration -> Global Configuration -> Wake on LAN -> Automatic Wake On LAN Proxy Detection** (default: off).
- Added: The thin client panel now contains a section **File Transfer Status** which gives status information about the assigned files.
- Added: New field **boot mode** in thin clients system information section.

Profiles

- Added: **Changes in UMS profiles can now be seen in their registry**. (Same colors as in the configuration tree).

Template Keys and Groups

- Added: **Static template keys**: For these template keys it is no longer necessary to configure and assign a template value since the thin client provides the values at runtime. The following three keys are available: MACADDRESS, HOSTNAME and UNITID. (Visible in each **Choose Template Key** dialog)

Firmware Customization

- Added: It is now possible to **assign wallpapers and boot splashes to W10 thin clients** (version 4.02.100 and higher) via firmware customizations.

Configuration Dialog

- Added: Additional **setup admin** user and permission layer on page **Accessories -> Setup -> User Page Permission**
- Added: Each parameter has got a new **reset button** which resets the value to factory defaults. The button is disabled when the parameter already has its default value.

Mobile Device Management (MDM)

- Added: **Mobile Device Management Preview**. Now it is possible to manage up to 5 mobile iOS devices with iOS version 10.3 or newer in the UMS.

UI / Look & Feel

- Added: If a tree node (folder, profile, master profile, firmware customization, view, ...) gets copied, and the target folder already contains an object with this name, the new displayed name will be marked with a **modifier ("COPY")**.

Resolved Issues 5.09.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UMS, Common

- Removed: **It is no longer possible to create UDC 2 licenses manually from smartcard** (Smartcard was directly connected to the UMS Console). It is still possible to configure and use a thin client as UDC 2 smartcard license server. (Automatic Licensing)
- Removed: **Support for SQL Server 2008 and SQL Server 2008 R2 databases**. (Incompatible SSL certificates)
- Fixed: Bug in **Automatic License Deployment** which occurred with **UD Pocket** devices. If the amount of registered unlicensed UD Pocket devices was higher than the amount of available licenses of one token, no license could be deployed.
- Fixed: **Automatic UDC2 license deployment created several identical licenses for the same thin client**.
- Fixed: **Offline user manual in UMS Console did not open on Linux OS**.
- Fixed: **install.log file** could not be added to the support information.
- Changed **default signature algorithm** for certificates to SHA512withRSA.
- Changed: The knowledge base links point now to kb.igel.com[48] instead of edocs.igel.com
- Changed: **Apache Tomcat** from version 8.0.47 to version 8.5.32.

Console, Common

- Removed: Unused graphical effects parameters for configuration dialog. (**UMS Console -> Misc -> Settings -> Configuration Dialog**)
- Fixed: **UMS Console window did not request focus anymore** while a firmware update is downloaded.
- Fixed: **Splash screen and accept certificate dialog can be hidden** behind other windows on Linux.
- Fixed: **Clearing the recycle bin** took much too long.
- Fixed: The **ID of non-displayable tree objects** is no longer shown with a thousands separator.
- Fixed: The **cache management dialog** in UMS Console did not open on Linux OS.
- Fixed: A **custom thin client attribute** which is linked to a default directory rule **could falsely be deleted**.
- Changed: **Users without the WebDav Access permission now get** a **more detailed hint** (message or tooltip) why they can´t perform some actions (e.g. creating a UMS file).
- Added: **All file choosers in the UMS Console can now remember their last used directory** (Except the WebDAV file choosers). This can be disabled in **UMS Console -> Misc -> Settings**.

Thin Clients

- Fixed: **User login history** had no entries for UD Pocket devices. (**UMS Console -> Management Tree -> Thin Clients -> Thin Client Content Panel**)

48 http://kb.igel.com

- Fixed: The actions **rename** and **delete** were selectable on the thin client root node. (**UMS Console -> Management Tree**)
- Fixed: After resetting a thin client to factory defaults, the **UMS Console still showed the thin client in the assigned objects**.
- Fixed: **After scanning several thin clients at once** (with specified target directory) **some of the scanned thin clients were not visible in the tree** until a refresh was done.
- Fixed: The thin **client settings cache** was not updated by assignment changes coming from administrative task **Assign profiles to the thin clients of views**.
- Fixed: Although the flag **Adjust network name if UMS-internal name has been changed** had been set, the thin client rename function ignored the maximum name length of 15 characters. (Rename via content panel)
- Fixed: The **Lock screen** icon (Advanced Thin Client Health Status) was permanently set if the thin client was remotely suspended.
- Changed: I**mproved usability** of thin client import dialog. (**UMS Console -> System -> Import -> Thin clients**)
- Changed: **Order of entries** in thin client context menu **Update & Snapshot Commands**.
- Changed: The **default thin client name** is now TC-MAC instead of IGEL-MAC to be fully DNS capable.

Profiles

- Fixed: Re-added missing file picker for field **file name** on page **System -> Update -> Snapshots -> Download**
- Fixed: Bug in **display configuration** where the second screen could not be saved on the left of screen one. (Only if both screen resolutions were set to **Autodetect**)

Template keys and groups

- Fixed: The **template check showed a missing value alert** (because no template value had been assigned to the thin client) although the setting in question had been overwritten by a correct profile/master profile and therefore did not affect the thin client.

Firmware Customization

- Fixed: **The config change flag in the thin client assignment panel was not displayed** if firmware customization was changed without sending the changes directly to the assigned thin clients.
- Fixed: In firmware Customizations, **the cancel button of the select file dialog did the same as the OK button**. When clicking the cancel button, changes will now be discarded instead of accepted.

Jobs

- Changed: Improved user interaction for **creating/editing a job where the execution time is in the past**.

Files

- Fixed: File **directories** could be renamed, but **after a refresh received the old name again**. (**UMS Console -> Management Tree -> Files**)

Configuration Dialog

- Fixed: The windows profile setting **Use IGEL Setup for configuration display settings** could be disabled, but after saving and reopening the configuration dialog, the **flag was still enabled**. (**Setup -> Configuration -> User Interface -> Display**)
- Fixed: **Huge memory consumption** in the configuration dialog of display page with high monitor resolutions.

Console, Administration Section

- Fixed: **Windows Server 2016 was not recognized as such**. OS name was displayed as "Windows NT (unknown)". (Visible in **UMS Console -> Administration Tree -> UMS Network -> Server -> Server Content Panel**)
- Fixed: Changes in the **Active Directory / LDAP** configuration didn't affect the management tree node **Shared Workplace Users** until the next connect.
- Fixed: **The thin client license node showed an access denied error on selection**, if the user had the permission to access the thin client license node, but not the UMS license node.
- Added: **Checkbox** to show only the last 20 executions in administrative task execution history to performance-friendly. (**UMS Console -> UMS Administration Tree -> Global Configuration -> Administrative Tasks**)
- Changed: **Configuration of concurrent thin client request threads** is now more user-friendly. (**UMS Console -> Administration Tree -> Global Configuration -> Thin Client Network Settings**)

Administrative Tasks

- Fixed: **Performance problem** which occurred if a newly created administration task with action **Delete logging data** had an incorrect export path set.
- Fixed: The two administrative tasks **Delete job execution data** and **Delete administrative job execution data** had wrong default values (Keep no more than x executions per job).
- Fixed: The administrative task **Delete job execution data** was not able to handle a very large amount of database entries (several millions).
- Fixed: A few 'old' administrative tasks could not be opened/reconfigured anymore.

IGEL Cloud Gateway (ICG)

- Fixed: The **usage date of mass-deployment keys** was not set. (**UMS Console -> Administration Tree -> Global Configuration -> Cloud Gateway Options**)
- Added: **Remote installer** for IGEL Cloud Gateway

Asset Inventory Tracker (AIT)

- Fixed: Asset names in **Asset Inventory Tracker** weren't appropriately truncated
- Added: **New administration task** to delete outdated asset history data. (**UMS Console -> Administration Tree -> Global Configuration -> Administrative Tasks**)

Server, Common

- Fixed: Bug which led to **high CPU-load of the UMS Server**, if the **Advanced Health Check** was enabled (**UMS Console -> Misc -> Settings -> Appearance**).

Administrator Application

- Fixed: The action **restore from backup** failed and the user got an error message. After the user acknowledged it, a wrong message **Database successfully restored** was displayed.
- Fixed: **Error while copying data into an oracle database**. (Only if **Asset Inventory Tracker** was used)
- Fixed: The **UMS Administrator database copy action aborted in some cases** (depending on the values in the database) with the following error: 'An attempt was made to get a data value of type 'BINARY' from a data value of type 'BLOB' '.
- Changed: **It is no longer possible to create a separate certificate backup in UMS Administrator**. The certificates are now contained in the database backup. The certificates (UMS to thin client communication) can be imported/exported in the new tree node **Certificate Management**. (**UMS Console -> Administration Tree -> Global Configuration**)

Installer (Linux)

- Added: Support for **Ubuntu 18.04**

UI / Look & Feel

- Fixed: **Broken row-sorter** in the license section
- Changed: **New Splash Screen** for UMS Console and UMS Administrator
- Changed: The UMS Console and UMS Administrator received **new task bar icons** and **application icons**.

Notes for Release 5.08.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Software:	Version	5.08.120
Release Date:	2018-06-22	
Release Notes:	Version	RN-508120-1
Last update:	2018-06-22	

The following formatting is used in this document:

format type	example	use
bold and underlined	enable/disable	the default setting of a value
bold and arrow	**menu > path**	menu path in the IGEL setup
bold	**GUI** [keyboard]	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	**[session name]**	variable values

Supported Environment 5.08.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)
Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **UMS Client:**

Microsoft Windows 7	(32 bit) (64 bit)
Microsoft Windows 8	(64 bit)
Microsoft Windows 10	(64 bit)
Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)
Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **Backend database (DBMS):**

Oracle 11g R2	(with RAC support)
Oracle 12c	(with RAC support)
Microsoft SQL Server 2008	
Microsoft SQL Server 2008 R2	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL 9.3 - 9.6 and 10.1	
Apache Derby 10	

Resolved Issues 5.08.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UMS (common)

- Fixed: Automatic UDC2 deployment creates unnecessarily several identical licenses for the same thin client. (Did not influence the smartcard license amount)

Notes for Release 5.08.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Software:	Version	5.08.110
Release Date:	2018-05-11	
Release Notes:	Version	RN-508110-1
Last update:	2018-05-11	

The following formatting is used in this document:

format type	example	use
bold and underlined	enable/disable	the default setting of a value
bold and arrow	**menu > path**	menu path in the IGEL setup
bold	**GUI** [keyboard]	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	**[session name]**	variable values

Supported Environment 5.08.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)
Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **UMS Client:**

Microsoft Windows 7	(32 bit) (64 bit)
Microsoft Windows 8	(32 bit) (64 bit)
Microsoft Windows 10	(32 bit) (64 bit)
Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)
Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **Backend database (DBMS):**

Oracle 11g R2	(with RAC support)
Oracle 12c	(with RAC support)
Microsoft SQL Server 2008	
Microsoft SQL Server 2008 R2	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
Microsoft SQL Server 2017	(with Cluster Support)
PostgreSQL 9.3 - 9.6 and 10.1	
Apache Derby 10	

New Features 5.08.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UMS (common)

- Added: This UMS version is licensed under a **new end user license agreement (EULA)**. Please read it carefully!

Resolved Issues 5.08.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UMS (common)

- Fixed: A **custom thin client attribute** which is linked to a default directory rule could falsely be deleted.
- Fixed: Bug in **Automatic License Deployment** which occurred with UD Pocket devices. If the number of registered unlicensed UD Pocket devices was higher than the number of available licenses of one token, no license could be deployed.
- Fixed: The **thin client settings cache** has not been updated by assignment changes coming from the administration task **Assign profiles to the thin clients of views**.

Console (common)

- Fixed: **UMS Console window doesn't request focus** anymore while a firmware update is downloaded.
- Fixed: Although the flag **Adjust network name if UMS-internal name has been changed** has been set, the **thin client rename function** ignored the maximum name length of 15 characters. (Rename via content panel)
- Fixed: **Cache management dialog in UMS Console** did not open on Linux.
- Fixed: **Offline user manual** in UMS Console did not open on Linux.

Console (administration section)

- Fixed: A few 'old' **administrative tasks** could not be opened/ reconfigured anymore.

Profiles

- Fixed: Bug in the **display configuration** where the second screen could not be saved on the left of screen one. (Only if both screen resolutions are set to 'Autodetect').

Configuration Dialog

- Fixed: The Windows profile setting **Use IGEL Setup for configuration display settings** could be disabled, but after saving and reopening the configuration dialog, the flag was still enabled. (**Setup > Configuration > User Interface > Display**).

Notes for Release 5.08.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Software:	Version	5.08.100
Release Date:	2018-01-29	
Release Notes:	Version	RN-508100-1
Last update:	2018-01-29	

The following formatting is used in this document:

format type	example	use
bold and underlined	enable/disable	the default setting of a value
bold and arrow	**menu > path**	menu path in the IGEL setup
bold	**GUI** [keyboard]	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	**[session name]**	variable values

Supported Environment 5.08.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

- **UMS Server:**

Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)
Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **UMS Client:**

Microsoft Windows 7	(32 bit) (64 bit)
Microsoft Windows 8	(64 bit)
Microsoft Windows 10	(64 bit)
Microsoft Windows Server 2008	(64 bit)
Microsoft Windows Server 2008 R2	(64 bit)
Microsoft Windows Server 2012	(64 bit)
Microsoft Windows Server 2012 R2	(64 bit)
Microsoft Windows Server 2016	(64 bit)
Ubuntu 14.04	(32 bit) (64 bit)
Ubuntu 16.04	(32 bit) (64 bit)
Oracle Linux 7	(64 bit)
Red Hat Enterprise Linux (RHEL) 6	(32 bit)
Red Hat Enterprise Linux (RHEL) 7	(64 bit)

- **Backend database (DBMS):**

Oracle 11g R2	(with RAC support)
Oracle 12c	(with RAC support)
Microsoft SQL Server 2008	
Microsoft SQL Server 2008 R2	
Microsoft SQL Server 2012	
Microsoft SQL Server 2014	(with Cluster Support)
Microsoft SQL Server 2016	(with Cluster Support)
PostgreSQL 9.3 - 9.6 and 10.1	
Apache Derby 10	

New Features 5.08.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Console (administration section)

- Added: **Automatic license deployment** for UDC3, UMA and UD Pocket. (**UMS Administration > Global Configuration > Licenses > Deployment**)

  If the feature is enabled (disabled by default) and appropriate tokens have been registered in the UMS, licenses for unlicensed UDC3 devices, UMA devices and UD Pockets are deployed automatically.

- Added: New tree node **Proxy Server** (**UMS Console > UMS Administration > Global Configuration**), to administrate several proxies in an easy way.
  As yet, a proxy could be configured for firmware updates only. A proxy now can be used for ICG´s and the new **Automatic License Deployment** feature too.

Thin Clients

- Added: **Snapshot upload/download support** for UMA devices with version 3.01.100 or higher.

Server (common)

- Changed: Because of security reasons, the **https connector of the UMS Server** does now provide **TLSv1.2** only.

UMS (common)

- Updated: **Apache Tomcat** version from 8.0.42 to **8.0.47**.
- Updated: **Java Version** from 1.8.0_121 to **1.8.0_152**.

Resolved Issues 5.08.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Console (common)

- Fixed: The **UMS Update Check** is now able to use a proxy. When a firmware update proxy is defined, the **Update Check** uses this proxy to verify whether there is a new UMS version available.
- Fixed: **Plenty wrong server log entries**. Occurred when the UMS user had no permission to see the license tree node in the **UMS Administration** tree and the **Advanced thin client health check** was active.
- Changed: Renamed the global permission **Snapshot** into **WebDAV access** (UMS file transfer).
- Changed: Users without the **WebDav Access** permission get now **a more detailed hint** (message or tooltip) why they cannot perform some actions (e.g. creating a UMS file).

Server (common)

- Fixed: Bug which led to high CPU load of the UMS server when the **Advanced Health Check** (**UMS Console > Misc > Settings > Appearance**) was enabled.
- Updated: PostgreSQL database driver to support **PostgreSQL v9.3 - v9.6 and v10**.

Firmware Customization

- Fixed: With **certain permission combinations**, users were not allowed **to assign files** to newly created firmware customizations.
- Fixed: **FileUpload via FWC-Wizard could lead to errors** when the user had insufficient permissions.
- Fixed: In **Firmware Customizations**, the **Cancel** button of the 'select file' dialog did the same as the **OK** button. By clicking the **Cancel** button, changes will now be discarded instead of accepted.

Universal Firmware Update

- Fixed: The **firmware update text viewer** remembers now its size, and the text font has been changed to a monospaced font to support text formation.

IGEL Cloud Gateway

- Fixed: **Root certificates** are now marked as a **certificate authority**.
- Fixed: After a connection to an **Igel Cloud Gateway** failed with a certificate error, some threads could not be closed.

Administrative Tasks

- Fixed: The **execution time of administration tasks** was reported to be in the past, although it was in the future.

> This issue occurred only for new or changed administrative tasks with execution time after 12:00 p.m. and before 12:00 a.m.

- Fixed: **Performance problem occurred** when a created administrative task with action **Delete logging data** got an incorrect export path set.

Console (administration section)

- Changed: Stored all license tree nodes into a new **Licenses** folder (**UMS > UMS Administration > Global Configuration**) and updated their icons.

Notes for Release 5.07.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Software:	Version	5.07.110
Release Date:	2017-10-19	
Release Notes:	Version	RN-507110-1
Last update:	2017-10-19	

The Linux installation was tested on the following distributions:

- Ubuntu 16.04 64-bit
- RedHat Enterprise 7.3
- Oracle Linux Server 7.3

The following formatting is used in this document:

format type	example	use
bold and underlined	enable/disable	the default setting of a value
bold and arrow	menu > path	menu path in the IGEL setup
bold	GUI keyboard	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	[session name]	variable values

Resolved Issues 5.07.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Console (common)

- Fixed: **Plenty server log entries** if the UMS user had no permission to see the license tree node in the UMS Administration and if the '**Advanced thin client health check**' was active.
- Fixed: **Firmware customizations could be manipulated** by a user without write permission.
- Changed: Renamed the global permission '**Snapshot**' into **WebDAV access (ums-filetransfer)**.

Firmware Customization

- Fixed: With certain permission combinations, users were not allowed to **assign files to newly created FWCs**.
- Fixed: **FileUpload via FWC-Wizard** could lead to errors if the user had insufficient permissions.

Administrative tasks

- Fixed: The **execution time of administration tasks** was reported to be in the past although it was in the future. This issue occurred only for new or changed administrative tasks with execution time after 12:00 p.m. and before 12:00 a.m.

AD / LDAP integration

- Fixed **AD login issue**: Login to UMS console failed with an AD user that had been indirectly imported to UMS via AD group. This issue occurred only if there was no browse user set in the AD configuration.

Notes for Release 5.07.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Software:	Version	5.07.100
Release Date:	2017-08-30	
Release Notes:	Version	RN-507100-1
Last update:	2017-08-30	

The following formatting is used in this document:

format type	example	use
bold and underlined	enable/disable	the default setting of a value
bold and arrow	**menu > path**	menu path in the IGEL setup
bold	**GUI** [keyboard]	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	**[session name]**	variable values

New Features 5.07.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UMS (common)

- Added: New Feature **Asset Inventory Tracker**.
  With a valid Asset Inventory license, it enables the user to collect Asset Inventory data from thin clients with Linux firmware 10.03.100 and higher.
  The data is displayed as part of the thin client details panel.

Console (common)

- Added: Function to **check for new UMS updates**. (**UMS > Help > UMS Update Check**)
- Added: **Export and import actions** for template keys, value groups, and firmware customizations.

Server (common)

- Updated: **Apache Tomcat** from version 8.0.41 to **8.0.44**.

Thin Clients

- Added: New thin client attribute **Battery Level**.
- Added: **Advanced thin client state icons**.
  The feature is activated by default and can be disabled via **Misc > Settings > Appearance > Use Advanced Health Status Icons**.
  In addition to the existing states (online and offline) four new states have been added: **Never communicated with UMS**, **License violated**, **In Lockscreen,** and **In Firmware Update**.
  The states **In Lockscreen** and **In Firmware Update** are only visible if the thin client firmware supports it and if the following option is set in the UMS (activated by default): **UMS Administration > Global Configuration > Thin Client Network > Thin Clients send updates**. This feature requires Linux firmware 10.03.100 or newer.
- Added: **Advanced message functionality**.
  The **Send Message** action in the thin client context menu opens a new editor to send customized messages and templates.
  Several default templates have been added and can be seen/changed in **UMS > UMS Administration > Global Configuration >TC Rich Message Templates**.
  Thin clients which do not support the feature are showing the plain message like before.
- Added: **Clear value button** for thin client attributes with type "DATE".

Universal Firmware Update

- Added: Filter option to show only the latest available firmware version in firmware update dialog. (**UMS Console > Universal Firmware Update Tree Node >** Context Menu **> Check for new firmware updates**)

Console (UMS Administration)

- Added: Possibility to use a list of **predefined thin client attribute values**. (**UMS Console > UMS Administration Tree > Global Configuration > Thin Client Attribute**)
- Changed: The **order of the tree nodes** in **UMS Console > UMS Administration > Global Configuration**.

Administrative Tasks

- Added: Administrative tasks can now be **executed monthly**.
- Added: New administration task to **save a UMS view on the file system**.

Firmwares

- Changed: Unused firmware can now be removed separately. (**UMS Console > Misc > Remove Unused Firmwares**)

IGEL Cloud Gateway (ICG)

- Changed: The **file and user synchronization process** after connecting an Igel Cloud Gateway is now executed in the **background**.

IGEL Management Interface (IMI)

- Added: IMI V3 supports now **Asset Inventory Information**.
- Added: IMI V3 supports now **Reset to factory defaults** for thin clients.
- Added: The thin client details do now contain the field **Battery Level** in IMI V3.

Installer (Linux)

- Added: Enhanced functionality for UMS installations on Linux. **Required libraries can now be installed automatically during UMS installation**.

Resolved Issues 5.07.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

UMS (common)

- Fixed: **Licenses can't be registered at the UMS** if the licenses are located on a network drive.
- Fixed: **UMS installations with more than three domain controllers** were not able to update to UMS version 5.05.100. After the update, each UMS login failed with a "truncation error" message.
- Fixed: The **Confirm deletion** dialog showed nested objects twice.
- Fixed: The **Restore backup** action failed for renamed `.pbak` backup files.
- Changed: If the internal thin client name is set to **overwrite the network name of the thin client**, there is now a check to make sure that the name is **DNS capable**.

Console (common)

- Changed: All **export actions** in the main menu are now always **enabled**, irrespective of the selected tree-object.
- Fixed: Bug in **UMS Linux installations** where hyperlinks could not be opened. (e.g. **UMS > UMS Administration > Misc Settings**)
- Added: The **thin client** content panel shows **icon corresponding to the current status** (online/offline/advanced health status)

Profiles

- Fixed: **Exporting profiles** (as archive) on a mapped network drive resulted in an unreadable file.
- Fixed: **Inconsistent results in profile comparison** when comparing two profiles in different directions (e.g. A-B vs B-A).

Template Keys and Groups

- Fixed: An error occurs if a template key or value group with **empty description** is edited and the **UMS database is an Oracle DB**.

Firmware Customization

- Fixed: **Display error in thin client directory assignments**. After a reload, the FWC assignments were not visible.
- Added: **FWC directories can now be copied** (including descendants).

Universal Firmware Update

- Fixed: Bug which was responsible for a **very low FTP firmware download rate**.

Configuration Dialog

- Fixed: After assigning two profiles (each with a default printer) to a thin client, the **thin client has now only one default printer set** (coming from a profile with higher priority).
- Fixed: **Coloring** for following changed and saved setup parameter:
  User Interface > Desktop
  Security > Logon > Active Directory / Kerberos
  Security > Smartcard > Middleware

Console (UMS Administrator)

- Fixed: After a change in **UMS Console > UMS Administration > Global Configuration > Server Network Settings > Broadcast IP** the user is not asked to save the change.
- Fixed: The **Igel Cloud Gateway configuration node** depended on permissions of Igel Cloud Gateway server node.
- Fixed: The dialog **Export all Unit IDs from a view** showed duplicated thin client entries in the result list. (**UMS Console > UMS Administration > Global Configuration > Thin Client Licenses > Export Unit ID list**)

Administrative Tasks

- Fixed: **Maximum amount of backups** has been ignored by database backup task.
- Fixed: The **reporting of a database backup job** showed a failed task even if the task was completed successfully.
- Changed: Handling of **immediate execution time** for administrative tasks.

AD / LDAP Integration

- Fixed: **Active Directory login error** for domain names without a separating dot.

IGEL Cloud Gateway (ICG)

- Fixed: **Reregistration of an ICG managed thin client** (before rebooting the ICG) leads to a connection error between the thin client and the ICG.
- Fixed: **UMS lost ICG connection** randomly.
- Fixed: Thin Client **license files could not be downloaded** via IGEL Cloud Gateway.
- Fixed: **File transfer via ICG fails** if a custom UMS file transfer folder location is used.
- Fixed: The **Igel Cloud Gateway configuration node** depended on permissions of Igel Cloud Gateway server node.
- Fixed: After an ICG administrated thin client got changed settings, **the configuration flag has not been cleared** for assigned objects (e.g. profiles).
- Fixed: The thin client **license upload fails** if the ICG license is expired.

Administrator Application

- Fixed: The **backups** section in the UMS Administrator was only active for embedded databases. Now the **backups** section is always enabled to give the possibility to create and restore certificates and server configurations with all databases.

Installer (Windows)

- Changed: To avoid incorrect input, **the backup file path in Windows installer can now only be set by the file chooser dialog**.

Installer (Linux)

- Fixed: Removed **irritating log4j warnings** during database backup process in Linux installer.
- Fixed: Removed **irritating jsvc_server.pid error** message in Linux installer summary.

UI / Look & Feel

- Added: **New splash screen** for UMS Console and UMS Administrator.

Fact Sheets

UMS Web App